МИНИСТЕРСТВО ЭКОНОМИЧЕСКОГО РАЗВИТИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ,
КАДАСТРА И КАРТОГРАФИИ
(РОСРЕЕСТР)

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ, КАДАСТРА И КАРТОГРАФИИ ПО ЧЕЛЯБИНСКОЙ ОБЛАСТИ

ПРИКАЗ

Челябинск

19 февраля 2019 г. № П/60

Об утверждении Политики информационной безопасности Управления Федеральной службы государственной регистрации, кадастра и картографии по Челябинской области

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К)», утвержденными приказом Гостехкомиссии от 30.08.2002 № 282, п р и к а з ы в а ю:

1. Утвердить Политику информационной безопасности Управления Федеральной службы государственной регистрации, кадастра и картографии по Челябинской области согласно приложению.

2. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель О.Ф. Смирных

ПРИЛОЖЕНИЕ

УТВЕРЖДЕНА

приказом Управления
Федеральной службы государственной
регистрации, кадастра и картографии
по Челябинской области
от 15 февраля 2023г № 11/60

ПОЛИТИКА

информационной безопасности Управления Федеральной службы государственной регистрации, кадастра и картографии по Челябинской области

1. Общие положения

1.1. Настоящая Политика информационной безопасности Управления Федеральной службы государственной регистрации, кадастра и картографии по Челябинской области (далее – Политика) на основании требований федеральных законов Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», постановления Правительства Российской Федерации от 03.11.94г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии», указов Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера», от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17

«Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», «Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)», утвержденных приказом Гостехкомиссии России от 30 августа 2002 г. № 282, и других нормативных правовых актов по защите информации.

1.2. Политика предназначена для обеспечения общих основ информационной безопасности и выбора практических мероприятий по обеспечению и управлению информационной безопасностью в Управлении Федеральной службы государственной регистрации, кадастра и картографии по Челябинской области (далее – Управление).

1.3. Работники Управления, ответственные за информационную безопасность, разрабатывают на объекты защиты Управления организационно-распорядительную документацию, дополняющую настоящую политику.

2. Объекты защиты

2.1. Объектами защиты Управления являются: информация, содержащаяся в информационных системах, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

3. Цели и задачи обеспечения информационной безопасности

3.1.Целью информационной безопасности является обеспечение непрерывности работы Управления при выполнении своих полномочий и

функций.

3.2.Указанная цель достигается посредством обеспечения и постоянного поддержания следующих основных свойств объектов защиты:

– конфиденциальность;

– целостность;

– доступность.

3.3.Необходимый уровень конфиденциальности, целостности и доступности обеспечивается соответствующими множеству значимых факторов, воздействующих на безопасность информации, мерами и средствами обеспечения информационной безопасности.

3.4.Задачами для достижения цели информационной безопасности являются:

– организация системы менеджмента информационной безопасности;

– своевременное выявление, оценка и прогнозирование факторов, воздействующих на безопасность информации, причин и условий, способствующих нарушению нормального функционирования информационных систем Управления;

– создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

– создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности;

– защита от несанкционированного доступа к объектам защиты;

– защита от несанкционированной модификации используемых в Управлении программных средств, а также защита информационных систем от внедрения несанкционированных программ, включая компьютерные вирусы;

– определение основных принципов информационной безопасности;

– определение мер и средств обеспечения информационной безопасности.

3.5. Поставленные цели и решение задач достигаются:

– строгим учетом всех объектов защиты;

– категорированием и классификацией объектов информатизации и информационных систем для обеспечения защиты на надлежащем уровне;

– регистрированием действий сотрудников Управления и организаций, осуществляющих обслуживание объектов защиты;

– распределением обязанностей по обеспечению информационной безопасности;

– выполнением всеми пользователями объектов защиты Управления требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности;

– персональной ответственностью за свои действия каждого сотрудника, имеющего доступ к объектам защиты Управления, в рамках своих функциональных обязанностей;

– повышением квалификации работников, ответственных за защиту информации в Управлении;

– систематической оценкой угроз;

– непрерывным поддержанием необходимого уровня информационной безопасности Управления;

– применением физических и технических (программно-аппаратных) средств защиты объектов защиты Управления;

– эффективным контролем над соблюдением пользователями объектов защиты Управления требований по обеспечению информационной безопасности.

4. Система менеджмента информационной безопасности

4.1. Система менеджмента информационной безопасности предназначена для создания, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы защиты информации в Управлении.

4.2. Основные принципы системы менеджмента информационной безопасности:

– понимание необходимости системы информационной безопасности;

– назначение ответственности за информационную безопасность;

– оценка риска, определяющая соответствующие меры и средства контроля и управления информационной безопасностью;

– обеспечение комплексного подхода к менеджменту информационной безопасности;

– выявление и предупреждение инцидентов информационной безопасности;

– непрерывная переоценка и соответствующая модификация системы информационной безопасности.

4.3. В целях непосредственной организации и эффективного функционирования системы менеджмента информационной безопасности на подразделение, отвечающее за обеспечение информационной безопасности в Управлении, возлагается решение следующих основных задач:

– реализация политики информационной безопасности, определение требований к системе защиты информации;

– анализ текущего состояния обеспечения информационной безопасности;

– контроль и оценка эффективности применяемых мер и средств защиты информации.

4.4. Основными функциями подразделения, отвечающего за обеспечение информационной безопасности в Управлении, являются:

– формирование требований к системам защиты в процессе создания и дальнейшего развития существующих объектов защиты;

– подготовка решений по обеспечению конфиденциальности, целостности, доступности объектов защиты;

– участие в проектировании систем защиты, их испытаниях и приемке в эксплуатацию;

– обеспечение функционирования установленных систем защиты информации, включая управление криптографическими системами;

– разграничение доступа пользователей к объектам защиты;

– проверка надежности функционирования системы защиты;

– разработка мер нейтрализации моделей возможных атак;

– обучение работников правилам безопасной обработки информации;

– контроль соответствия действий администраторов и пользователей установленным правилам обращения с информацией;

– участие в служебных проверках по фактам нарушений правил обращения с информацией и оборудованием в Управлении;

– сбор, накопление, систематизация и обработка информации по вопросам информационной безопасности.

5. Факторы, воздействующие на безопасность информации

5.1. Выявление и учет факторов, воздействующих на защищаемую информацию, составляют основу для планирования и проведения эффективных мероприятий по информационной безопасности.

5.2. Выявление факторов, воздействующих на безопасность информации, должно осуществляться с учетом следующих требований:

– достаточности уровней классификации факторов, позволяющих формировать их полное множество;

– гибкость классификации, позволяющей расширять множества классифицируемых факторов, а также вносить необходимые изменения без нарушения структуры классификации.

5.3. По отношению к объектам защиты факторы разделяются на внутренние и внешние.

5.4. Основными факторами, воздействующими на безопасность информации в Управлении являются:

– непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей объектов защиты Управления (в том числе работников,

отвечающих за обслуживание и администрирование), приводящие к непроизводительным затратам времени и ресурсов, разглашению, потере конфиденциальной информации или нарушению работоспособности объектов защиты;

– преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом, халатность и т.п.) действия легально допущенных к объектам защиты Управления пользователей (в том числе работников, отвечающих за обслуживание и администрирование), приводящие к непроизводительным затратам времени и ресурсов, разглашению, потере конфиденциальной информации или нарушению работоспособности объектов защиты Управления;

– деятельность преступных групп и формирований, политических и экономических структур, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности объектов защиты Управления;

– ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации и контроля эффективности защиты);

– явления техногенного характера, стихийные бедствия.

5.5. Реализация основных объективных факторов, воздействующих на безопасность информации, возможна путем:

– выхода из строя оборудования и программных средств объектов защиты Управления;

– выхода из строя или невозможность использования линий связи;

– пожаров, наводнений и других стихийных бедствий и явлений техногенного характера.

5.6. Реализация непреднамеренных субъективных факторов, воздействующих на безопасность информации, возможна путем:

– неумышленных действий, приводящих к частичному или полному нарушению функциональности компонентов или разрушению объектов защиты

Управления;

– неосторожных действий, приводящих к разглашению информации ограниченного распространения или делающих ее общедоступной;

– разглашения, передачи или утраты атрибутов разграничения доступа (пропусков, идентификационных карточек, ключей, паролей, ключей шифрования и т. п.);

– игнорирования организационных правил при работе с объектами защиты Управления;

– проектирования технологий обработки данных, разработки программного обеспечения с возможностями, представляющими опасность для функционирования информационных систем Управления и информационной безопасности;

– пересылки данных и документов по ошибочному адресу (устройства);

– ввода ошибочных данных;

– неумышленной порчи и утраты носителей информации;

– неумышленного повреждения каналов связи;

– неправомерного отключения оборудования или изменения режимов работы устройств или программ;

– заражения компьютеров вирусами;

– несанкционированного запуска технологических программ, способных вызвать потерю работоспособности информационных систем Управления или осуществляющих необратимые в них изменения (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

– некомпетентного использования, настройки или неправомерного отключения средств защиты.

5.7. Реализация преднамеренных субъективных факторов, воздействующих на безопасность информации, возможна путем:

– умышленных действий, приводящих к частичному или полному нарушению или разрушению объектов защиты Управления;

– хищения документов и носителей информации;

– несанкционированного копирования документов и носителей информации;

– умышленного искажения информации, ввода неверных данных;

– отключения или вывода из строя подсистем обеспечения функционирования объектов защиты Управления (электропитания, охлаждения и вентиляции, линий и аппаратуры связи и т.п.);

– перехвата данных, передаваемых по каналам связи, и их анализа;

– незаконного получения атрибутов разграничения доступа (агентурным путем, используя халатность пользователей, путем подделки, подбора и т.п.);

– хищения или вскрытия шифров криптозащиты информации;

– внедрения аппаратных и программных закладок с целью скрытного осуществления доступа к объектам защиты Управления;

– незаконного использования оборудования, программных средств или информационных ресурсов, нарушающее права третьих лиц;

– применения подслушивающих устройств, дистанционной фото- и видео съемки для несанкционированного съема информации.

6. Основные принципы информационной безопасности

6.1. При построении системы информационной безопасности Управления необходимо руководствоваться следующими основными принципами:

– законность (осуществление защитных мероприятий и разработки системы информационной безопасности Управления в соответствии с действующим законодательством в области защиты информации);

– системность (учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности);

– комплексность (согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные

каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов);

– непрерывность (постоянная работа и организационная поддержка мер и средств защиты для эффективного обеспечения информационной безопасности);

– своевременность (постановка задач по комплексной защите информации и реализация мер обеспечения информационной безопасности на ранних стадиях разработки информационных систем в целом и их систем защиты информации в частности);

– преемственность и непрерывность совершенствования (совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем и систем их защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите);

– разумная достаточность (выбор достаточного уровня защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми);

– персональная ответственность (ответственность за обеспечение информационной безопасности для каждого сотрудника Управления в пределах его полномочий);

– взаимодействие и сотрудничество (сотрудники Управления должны осознанно соблюдать установленные правила и оказывать содействие деятельности подразделений (ответственных лиц) за обеспечение информационной безопасности);

– гибкость системы защиты (способность реагировать на изменения внешней среды и условий осуществления Управлением своих функций);

– простота применения средств защиты (не должно быть связано с выполнением действий, требующих значительных дополнительных трудозатрат при работе пользователей);

– обоснованность и техническая реализуемость (обоснованность с точки

зрения достижения заданного уровня безопасности информации, а также соответствие установленным нормам и требованиям по безопасности информации);

– специализация и профессионализм (реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными сотрудниками Управления);

– обязательность контроля (обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения информационной безопасности на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств).

7. Меры и средства обеспечения информационной безопасности

7.1. При осуществлении менеджмента информационной безопасности необходимо выделить следующие основные меры обеспечения информационной безопасности:

– законодательные (законодательство Российской Федерации в сфере информационной безопасности). Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с сотрудниками Управления;

– морально-этические (нормы поведения, которые сложились или складываются по мере распространения информационных технологий в обществе). Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в Управлении;

– технологические (технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками Управления ошибок и нарушений в рамках предоставленных им прав и полномочий);

– организационные (меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность сотрудников Управления, а также порядок взаимодействия пользователей с объектами защиты Управления таким образом, 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 разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для предотвращения несанкционированного доступа к объектам защиты, а также технических средств визуального наблюдения, связи и охранной сигнализации);

– технические (меры защиты основаны на использовании различных электронных устройств и специального программного обеспечения, выполняющих функции защиты).

7.2. Для обеспечения информационной безопасности необходимо использовать средства:

– физической защиты (введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки конфиденциальной информации, оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи);

– антивирусной защиты (предотвращение потерь, ошибок и модификации информационных ресурсов);

– резервирования (поддержание целостности и доступности объектов защиты);

– разграничения доступа (управление доступом к информационным ресурсам, к сети общего пользования, к локальной вычислительной сети);

– криптографической защиты (защита конфиденциальности, целостности и аутентичности информационных ресурсов путем применения средств

криптографической защиты информации, в том числе при передаче по каналам связи);

– идентификации и аутентификации (предотвращение работы с информационными ресурсами посторонних лиц путем обеспечения возможности распознавания каждого легального пользователя);

– контроля целостности (своевременное обнаружение модификации или искажения информационных ресурсов, обеспечение правильности функционирования системы защиты и целостности хранимой и обрабатываемой информации);

– контроля и регистрации событий информационной безопасности (обеспечение обнаружения и регистрации всех событий, которые могут повлечь за собой нарушение информационной безопасности).

8. Ответственность за нарушение обеспечения информационной безопасности

8.1. Нарушение информационной безопасности может повлечь дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.