Учреждение образование

«Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

Основы защиты информации

Политика информационной безопасности

юридической компании OAO «Законник»

Выполнила: Керезь Екатерина, 4 группа, 2 курс

Принял: Буснюк Николай Николаевич

Минск 2020

**Оглавление**

[Введение 3](#_Toc34996605)

[1. Общие положения 3](#_Toc34996606)

[1.2 Структура компании и организация связи 4](#_Toc34996607)

[1.3 Возможные угрозы и их анализ 4](#_Toc34996608)

[2.1 Исследование политики безопасности компании 6](#_Toc34996609)

[2.2 Организационный элемент защиты информации на OAO «Законник» 7](#_Toc34996610)

[2.3 Нормативно-правовой элемент защиты информации на предприятии OAO «Законник» 8](#_Toc34996611)

[2.4 Инженерно-технический элемент защиты информации на OAO «Законник» 9](#_Toc34996612)

[3. Политика информационной безопасности 11](#_Toc34996613)

[3.1 Политика предоставления доступа к информационному ресурсу 11](#_Toc34996614)

[3.2 Политика учетных записей 11](#_Toc34996615)

[3.3 Политика архивирования, резервного копирования и восстановления данных 12](#_Toc34996616)

[3.4 Политика реализации антивирусной защиты 12](#_Toc34996617)

[3.5 Политика защиты автоматизированного рабочего места (АРМ) 13](#_Toc34996618)

[3.6 Политика пользования электронной почтой 14](#_Toc34996619)

[Заключение 15](#_Toc34996620)

## Введение

Информация – один из наиболее важных ресурсов в современном мире.

Каждая компания сталкивается с необходимостью управлять и организовывать огромные объемы передачи информации. По этой причине, одним из главных направлений при развитии компании является направленность на политику безопасности.

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

Компания ОАО «Законник» хранит персональные данные своих клиентов и сотрудников. Компания обеспечивает безопасность и устойчивость информационной безопасности за счет денежных вложений в политику безопасности.

Исследование проблемы информационной безопасности в данной компании так же связано с тем, что хранимая информация крайне конфиденциальна и требует абсолютной защиты от посторонних лиц.

Защита баз данных, хранящих практически всю информацию о клиентах и сотрудниках, является сложной, но обязательной задачей, без решения которой невозможно качественное обслуживание клиентов компании.

## 1. Общие положения

Информация является ценным и жизненно важным ресурсом OAO «Законник» (далее – Компания). Настоящая политика информационной безопасности предусматривает принятие необходимых мер в целях защиты активов от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в Компании.

Ответственность за соблюдение информационной безопасности несет каждый сотрудник Компании, при этом первоочередной задачей является обеспечение безопасности всех активов Компании. Это значит, что информация должна быть защищена не менее надежно, чем любой другой основной актив Компании. Главные цели Компании не могут быть достигнуты без своевременного и полного обеспечения сотрудников информацией, необходимой им для выполнения своих служебных обязанностей.

1.2 Структура компании и организация связи

Основным документом, регламентирующим [корпоративное управление](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D1%80%D0%BF%D0%BE%D1%80%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D0%B5_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5) в ОАО «Законник», является его устав. Согласно уставу, высшим органом управления общества является собрание директоров, которое проводится не реже раза в год. В состав исполнительных органов Компании входит коллегиальный исполнительный орган — правление.

В компании действует следующая система управления: стратегические и операционные функции поделены между корпоративным центром и филиалами. В ОАО «Законник» приняты кодексы этических норм и кодекс корпоративного поведения.

Информационные системы, на которых работает компания, в данном случае, образуются совокупностью оборудования сетей центрального офиса, филиалов и кабинетов пользователей.

## 1.3 Возможные угрозы и их анализ

Угроза безопасности, потенциальное нарушение безопасности, любое обстоятельство или событие, которое может является причиной нанесения ущерба предприятию в целом.

Все множество потенциальных угроз по природе их возникновения разделяется на два класса: естественные (объективные) и искусственные (субъективные).

Естественные угрозы — это угрозы, вызванные воздействиями на предприятие объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы — это угрозы предприятию, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

* непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;
* преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).

Источники угроз по отношению к предприятию могут быть внешними или внутренними (составляющие самой организации - её аппаратура, программы, персонал, конечные пользователи).

Основные непреднамеренные искусственные угрозы предприятию (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

* неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);
* неправомерное отключение оборудования или изменение режимов работы устройств и программ;
* неумышленная порча носителей информации;
* запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
* нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
* заражение компьютера вирусами;
* неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;
* разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
* проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
* игнорирование организационных ограничений (установленных правил) при работе в системе;
* некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
* пересылка данных по ошибочному адресу;
* ввод ошибочных данных;
* неумышленное повреждение каналов связи.

Основные возможные пути умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

* внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);
* вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
* применение подслушивающих устройств, дистанционная фото- и видео-съемка и т.п.;
* перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сели питания, отопления и т.п.);
* перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;
* хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ);
* несанкционированное копирование носителей информации;
* хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
* чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
* чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой зашиты) или другими пользователями, в асинхронном режиме используя недостатки мультизадачных операционных систем и систем программирования;
* незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);
* несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;
* вскрытие шифров криптозащиты информации;
* внедрение аппаратных «спецвложений», программных «закладок» и «вирусов» («троянских коней» и «жучков»), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;

Следует заметить, что чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

**2. Исследование процессов защиты информации в компании OAO «Законник»**

## 2.1 Исследование политики безопасности компании

Политика безопасности — это документ «верхнего» уровня, в котором должно быть указано:

* ответственные лица за безопасность функционирования фирмы;
* полномочия и ответственность отделов и служб в отношении безопасности;
* организация допуска новых сотрудников и их увольнения;
* правила разграничения доступа сотрудников к информационным ресурсам;
* организация пропускного режима, регистрации сотрудников и посетителей;
* использование программно-технических средств защиты;
* другие требования общего характера.

Особое внимание в политике безопасности надо уделить разграничению зоны ответственности между службой безопасности и IT-службой предприятия. Зачастую сотрудники службы безопасности, в силу низкой технической грамотности, не осознают важности защиты компьютерной информации. С другой стороны, IT-сотрудники, являясь «творческими» личностями, как правило, стараются игнорировать требования службы безопасности.

Для защиты информации на предприятии OAO «Законник» разработана система защиты информации (СЗИ). В которой выделяют следующие элементы СЗИ:

* организационный элемент Защиты информации (ЗИ) - включает регламентацию производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающую или ослабляющую нанесение, какого-либо ущерба исполнителям. На данном предприятии имеется шлагбаум при въезде на территорию, въезд осуществляется только по пропускам, на окнах первого этажа имеются решетки, ведется видеонаблюдение за всей территорией предприятия;
* нормативно-правовой элемент ЗИ — это специальные законы, акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе. На данном предприятии существуют: правила внутреннего распорядка, санитарные правила, правила пожарной безопасности;
* инженерно-технический элемент ЗИ — это использование различных инженерно-технических средств, препятствующих нанесению ущерба защищаемой информации;
* программно-аппаратный элемент ЗИ — это все программные и автоматизированные системы обработки данных, обеспечивающие сохранность и конфиденциальность информации.

## 2.2 Организационный элемент защиты информации на OAO «Законник»

Организационная защита информации на предприятии - регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

Организационная защита информации:

* организация работы с персоналом;
* организация внутриобъектового и пропускного режимов и охраны;
* организация работы с носителями сведений;
* комплексное планирование мероприятий по защите информации;
* организация аналитической работы и контроля.

Основные принципы организационной защиты информации:

* принцип комплексного подхода - эффективное использование сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой информации;
* принцип оперативности принятия управленческих решений (существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает нацеленность руководства и персонала предприятия на решение задач защиты информации);
* принцип персональной ответственности - наиболее эффективное распределение задач по защите информации между руководством и персоналом предприятия и определение ответственности за полноту и качество их выполнения.

Среди основных условий организационной защиты информации можно выделить следующие:

* непрерывность всестороннего анализа функционирования системы защиты информации в целях принятия своевременных мер по повышению ее эффективности;
* неукоснительное соблюдение руководством и персоналом предприятия установленных норм и правил защиты конфиденциальной информации.

При соблюдении перечисленных условий обеспечивается наиболее полное и качественное решение задач по защите конфиденциальной информации на предприятии.

## 2.3 Нормативно-правовой элемент защиты информации на предприятии OAO «Законник»

Правовой элемент системы организации защиты информации на предприятии OAO «Законник» основывается на нормах информационного права и имеет юридическое закрепление взаимоотношений фирмы и государства по поводу правомерности использования системы защиты информации, фирмы и персонала по поводу обязанности персонала соблюдать установленные меры защитного характера, ответственности персонала за нарушение порядка защиты информации.

Этот элемент включает:

* наличие в организационных документах фирмы, правилах внутреннего трудового распорядка, трудовых договорах, в должностных инструкциях положений и обязательств по защите конфиденциальной информации;
* формулирование и доведение до сведения всех сотрудников положения о правовой ответственности за разглашение конфиденциальной информации, несанкционированное уничтожение или фальсификацию документов;
* разъяснение лицам, принимаемым на работу, положения о добровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите информации.

В числе основных подсистем защиты информации в правовом плане можно считать:

* установление на объекте режима конфиденциальности;
* разграничение доступа к информации;
* правовое обеспечение процесса защиты информации;
* четкое выделение конфиденциальной информации как основного объекта защиты.

Опираясь на государственные правовые акты на уровне OAO «Законник», разрабатываются собственные нормативно-правовые документы, ориентированные на обеспечение информационной безопасности.

К таким документам относятся:

* политика Информационной безопасности;
* положение о защите персональных данных;
* перечень сведений, составляющих конфиденциальную информацию;
* инструкция о порядке допуска сотрудников к сведениям, составляющим конфиденциальную информацию;
* положение о специальном делопроизводстве и документообороте;
* обязательство сотрудника о сохранении конфиденциальной информации;
* памятка сотруднику о сохранении коммерческой тайны.

Указанные нормативные акты направлены на предупреждение случаев неправомерного оглашения (разглашения) секретов на правовой основе, и в случае их нарушения должны приниматься соответствующие меры воздействия.

## 2.4 Инженерно-технический элемент защиты информации на OAO «Законник»

Инженерно-технический элемент защиты информации предназначен для пассивного и активного противодействия средствам технической разведки и формирования рубежей охраны территории, зданий, помещений и оборудования с помощью комплексов технических средств.

Организация охраны - составная часть общей системы защиты конфиденциальной информации предприятия. Вопросы обеспечения надежной охраны территории предприятия и его объектов неразрывно связаны с задачами организации пропускного режима на предприятии. Силы и средства, участвующие в решении этих задач, являются составными элементами системы охраны предприятия.

От эффективности функционирования системы охраны в полной мере зависят возможность и уровень решения задач пропускного и внутриобъектового режимов. Системы пропускного и внутриобъектового режимов образуют следующие после системы охраны рубежи безопасности, предотвращающие доступ злоумышленника к охраняемой предприятием информации.

Главные цели охраны OAO «Законник» следующие:

* обеспечение сохранности находящихся на охраняемой территории носителей конфиденциальной информации и материальных средств и исключение, таким образом, нанесения ущерба предприятию;
* предупреждение происшествий на охраняемом объекте и ликвидация их последствий.

К основным объектам охраны относятся:

территория компании;

* носители конфиденциальной информации (документы, изделия);
* материальные ценности.

Особыми объектами охраны является руководство предприятия и персонал, допущенный к конфиденциальной информации. Организация охраны руководства и персонала предприятия регулируются отдельным положением, которое утверждается руководителем предприятия, и, в необходимых случаях согласовывается с территориальными органами внутренних дел и органами безопасности. Основные цели охраны руководства и перевала предприятия - обеспечение их личной безопасности в повседневных условиях и при возникновении чрезвычайных ситуаций, предотвращение возможных попыток завладения злоумышленниками защищаемой информацией путем физического и иного насильственного воздействия на этих лиц, выработка рекомендаций охраняемым лицам по особенностям поведения в различных ситуациях.

1. Политика информационной безопасности
   1. Политика предоставления доступа к информационному ресурсу

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к защищаемым информационным ресурсам Управления.

К работе с информационным ресурсом допускаются пользователи, ознакомленные с правилами работы с информационным ресурсом и ответственностью за их нарушение, а также настоящей политикой.

Каждому сотруднику Управления, допущенному к работе с конкретным информационным ресурсом, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.

В случае необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в Управлении одного и того же имени пользователя («группового имени») ЗАПРЕЩЕНО.

3.2 Политика учетных записей

Настоящая политика определяет основные правила присвоения учетных записей пользователям информационных активов компании.

Регистрационные учетные записи подразделяются на:

* пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов Управления;
* системные – используемые для нужд операционной системы;
* служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов Управления назначается 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.

* 1. Политика архивирования, резервного копирования и восстановления данных

Требования к архивированию, резервному копированию и восстановлению данных определяется уровнем риска сервиса, требованием к доступности сервиса и устанавливаются следующие:

Режим работы сервиса Интернет круглосуточный, время восстановления 2 часа (не по вине провайдера, предоставляющего доступ к сети)

Режим работы электронной почты круглосуточный, время восстановления 4 часа (не по вине провайдера, предоставляющего доступ к сети)

Режим работы файлового архива круглосуточный, время восстановления 4 часа.

Режим работы системы по управлению предприятием круглосуточный, время восстановления 4 часа. Полное ежедневное копирование базы данных и хранение в течение 30 дней. 2 раза в год полное копирование и хранение в течение 5 лет.

* 1. Политика реализации антивирусной защиты

Настоящая Политика определяет основные правила для реализации антивирусной защиты в Управлении.

Антивирусное программное обеспечение должно быть установлено, настроено и активировано на всех программно-технических средствах, имеющих доступ к информационным активам ОАО «Законник», до начала их использования или подключения к информационным ресурсам.

Все возможные каналы поступления вредоносного программного обеспечения в информационно-технологическую инфраструктуру организации должны быть определены, проанализированы и защищены средствами антивирусной защиты.

Контролю на предмет обнаружения вредоносных программ должна подвергаться вся информация, создаваема и обрабатываемая программно-техническими средствами ОАО «Законник», а также принимаемая (передаваемая) посредством сменных носителей информации и средствами телекоммуникаций.

С целью эффективной борьбы с новыми видами зловредного программного обеспечения и уменьшения накладных расходов на администрирование должно выполняться централизованное, регулярное обновление всех средств антивирусной защиты, используемых для защиты информационных систем организации.

Для эффективной реализации АВЗ ОАО «Законник», необходимо:

* унифицировать антивирусное программное обеспечение с возможностью централизованного управления
* постоянное, своевременное обновление антивирусных баз и программных компонентов

Реализацию данного пункта политики безопасности осуществляет системный администратор, контроль за исполнением обеспечивает заведующий отделом ИТ.

* 1. Политика защиты автоматизированного рабочего места (АРМ)

Настоящая Политика определяет основные правила и требования по защите персональных данных и иной конфиденциальной информации Управления от неавторизованного доступа, утраты или модификации.

Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами.

При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу или ящике стола или в сейфе.

Несанкционированное использование печатающих, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.

Сотрудники получают доступ к ресурсам вычислительной сети после ознакомления с документами, утвержденными стандартами Управления, (согласно занимаемой должности), а именно с инструкциями по обращению с носителями конфиденциальной информации, «Перечень сведений конфиденциального характера».

Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только администратор информационной безопасности. Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.

Доступ к информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

Пользователям запрещается устанавливать неавторизованные программы на компьютеры.

Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ.

Техническое обслуживание должно осуществляться только на основании обращения пользователя к системному администратору.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.

Программное обеспечение должно устанавливаться со специальных ресурсов или съемных носителей и в соответствии с лицензионным соглашением с его правообладателем.

Системный администратор вправе отказать в устранении проблемы, вызванной наличием на рабочем месте программного обеспечения или оборудования, установленного или настроенного пользователем в обход действующей процедуры.

## 3.6 Политика пользования электронной почтой

Электронная почта – используется только для выполнения работником его служебных обязанностей.

Единственно возможный способ работы с электронной почтой в ОАО «Законник» – использование корпоративной электронной почты. Работа с другими сервисами электронной почты, включая, но не ограничиваясь, бесплатными почтовыми серверами, только при согласовании с системным администратором организации.

Запрещается рассылка цепных сообщений, спама, исполняемых файлов, файлов развлекательного характера.

Запрещается использовать корпоративную электронную почту для любой деятельности с целью получения личной материальной выгоды.

Запрещается пересылка и получение электронной почты, содержащей лицензионное программное обеспечение и другие действия, позволяющие обойти лицензионные соглашения или нарушить авторские права

Запрещается посылать письма, содержащие информацию, составляющие коммерческую тайну ОАО «Законник». Исключения составляют пользователи, имеющие на это право в соответствии с положением «О коммерческой тайне»

## Заключение

В современном мире стремительно быстро развиваются новые технологии, так же быстро и появляются новые устройства, методы для кражи информационных ресурсов. У любого предприятия, дорожащего своей репутацией и прибылью, должна быть чётко сформирована система защиты, как информации, так и предприятия в целом. На таком предприятии, как ОАО «Законник» утечка данных может привести не только к краху корпорации, но и нанести ущерб клиентам компании, так как в автоматизированной системе организации находятся персональные данные клиентов, включающие паспортные данные, которые должны храниться в секрете от посторонних лиц.