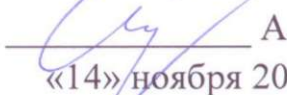


Общество с ограниченной ответственностью «Бауцентр Рус»

УТВЕРЖДАЮ

Генеральный директор
ООО «Бауцентр РУС»


А.Ю. Курандин
«14» ноября 2017 г.



Политика информационной безопасности

г. Калининград
2017 г.

Настоящая **Политика информационной безопасности** (далее – **Политика Общества с ограниченной ответственностью «Бауцентр Рус»** (далее - ООО «Бауцентр Рус»)), разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных и является официальным документом.

Политика разработана в соответствии с требованиями:

- ❖ Федерального закона Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- ❖ Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- ❖ Постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- ❖ Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных»;
- ❖ приказа ФСТЭК России от 18 Февраля 2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

В **Политике** определены требования к работникам, допущенных для работы в информационных системах персональных данных (далее – ИСПДн), степень ответственности данных работников, структура и необходимый уровень защищенности ИСПДн ООО «Бауцентр Рус», статус и должностные обязанности работников, ответственных за обеспечение безопасности персональных данных (далее – ПДн) в ИСПДн ООО «Бауцентр Рус».

1. Общие положения

Целью настоящей **Политики** является:

- ✓ обеспечение безопасности объектов защиты ООО «Бауцентр Рус» от всех видов угроз (внешних, внутренних, умышленных, непреднамеренных);
- ✓ минимизация ущерба от возможной реализации угроз безопасности персональных данных (далее - УБПДн).

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей.

В ООО «Бауцентр Рус» осуществляется своевременное обнаружение и реагирование на УБПДн, предотвращение преднамеренных или случайных, частичных, или полных несанкционированных модификаций, или уничтожения данных.

Состав объектов защиты утвержден приказами генерального директора ООО «Бауцентр Рус»:

- ❖ «О проведении работ по обеспечению безопасности персональных данных, об утверждении перечня информационных систем персональных данных, контролируемой зоны помещений, инструкций, форм журналов, назначении администратора информационной безопасности»;
- ❖ «Об утверждении Положения, инструкций по информационной безопасности, форм журналов, об определении мест хранения материальных носителей».

Состав персональных данных, обрабатываемых в ИСПДн, подлежащих защите, утвержден приказом генерального директора ООО «Бауцентр Рус»:

- ❖ «Об утверждении списка лиц, имеющих доступ к персональным данным, постоянных пользователей информационных систем персональных данных, допущенных в помещения, прав доступа к информационным и техническим ресурсам, перечня персональных данных, подлежащих защите».

Политика утверждена приказом генерального директора ООО «Бауцентр Рус»:

- ❖ «Об утверждении организационно-распорядительной документации, относящейся к системе защиты персональных данных».

Требования настоящей **Политики** распространяются на всех работников ООО «Бауцентр Рус» (штатных, работающих по различным видам договоров и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

2. Система защиты персональных данных

Система защиты персональных данных в ООО «Бауцентр Рус» (далее - СЗПДн), строится на основании:

- ✓ аналитических отчетов по результатам обследования информационных систем персональных данных (далее – Аналитический отчет);
- ✓ частных моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- ✓ перечня персональных данных, подлежащих защите;
- ✓ актов определения уровня защищенности персональных данных, при их обработке в информационных системах персональных данных;
- ✓ локальных актов ООО «Бауцентр Рус»;
- ✓ организационно-распорядительной документации относящейся к системе защиты информации и персональных данных.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн ООО «Бауцентр Рус».

На основании анализа актуальных угроз безопасности ПДн описанных в частных моделях угроз безопасности персональных данных, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн.

Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению безопасности персональных данных ООО «Бауцентр Рус». План мероприятий по обеспечению безопасности персональных данных утверждается приказом генерального директора ООО «Бауцентр Рус».

Для каждой ИСПДн в Аналитических отчетах составляется перечень используемых технических средств, программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн, включающих в себя:

- ✓ перечень основных технических средств (далее – ОТСС);
- ✓ перечень вспомогательных технических средств, располагаемых совместно с ОТСС;
- ✓ перечень программного обеспечения, используемого в ИСПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства защиты информации (далее – ТСЗИ):

- ✓ антивирусные средства для рабочих мест пользователей и серверов;
- ✓ средства защиты информации от несанкционированного доступа;
- ✓ средства межсетевое экранирования;
- ✓ средства технической защиты информации, используемые для защиты информации от несанкционированного доступа;
- ✓ средства криптографической защиты информации, используемые при передаче защищаемой информации по открытым каналам связи.

3. Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие подсистемы:

- ✓ управления доступом, регистрацией и учетом;
- ✓ обеспечения целостности и доступности;
- ✓ антивирусной защиты;
- ✓ межсетевое экранирования;
- ✓ анализа защищенности;
- ✓ обнаружения вторжений;
- ✓ отсутствие не декларированных возможностей.

Подсистемы СЗПДн имеют различный функционал в зависимости от определенных уровней защищенности ИСПДн, определенного в акте определения уровня защищенности персональных данных, при их обработке в информационной системе персональных данных.

4. Пользователи ИСПДн

В ИСПДн ООО «Бауцентр Рус» выделены следующие группы пользователей, участвующих в обработке и хранении ПДн:

- ✓ пользователи, имеющих доступ к персональным данным, в части выполнения своих должностных обязанностей;
- ✓ пользователи, непосредственно участвующие в обработке персональных данных, в части выполнения своих должностных обязанностей.

Данные о пользователях, уровне их доступа и информированности утверждены приказом по ООО «Бауцентр Рус»:

- ❖ **«Об утверждении списка лиц, имеющих доступ к персональным данным, постоянных пользователей информационных систем персональных данных, допущенных в помещения, прав доступа к информационным и техническим ресурсам, перечня персональных данных, подлежащих защите».**

Контроль за выполнение технических мероприятий по обеспечению безопасности персональных данных возлагается на администратора информационной безопасности (далее – администратор ИБ).

Администратор ИБ назначен приказом генерального директора ООО «Бауцентр Рус»:

- ❖ **«О проведении работ по обеспечению безопасности персональных данных, об утверждении перечня информационных систем персональных данных, контролируемой зоны помещений, инструкций, форм журналов, назначении администратора информационной безопасности».**

4.1. Администратор информационной безопасности

Администратор ИБ, штатный работник ООО «Бауцентр Рус», ответственный за функционирование СЗПДн, включая обслуживание и настройку клиентской составляющей.

Администратор ИБ обладает следующим уровнем доступа и знаний:

- ✓ обладает полной информацией об ИСПДн;
- ✓ имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.

Администратор ИБ уполномочен:

- ✓ реализовывать политику безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (оператор АРМ) получает возможность работать с элементами ИСПДн;
- ✓ осуществлять аудит средств защиты;
- ✓ устанавливать доверительные отношения своей защищенной сети с сетями других организаций и учреждений;

- ✓ осуществлять внутренние проверки режима защиты персональных данных в информационных системах персональных данных и фиксировать в «Журнале внутренних проверок режима защиты персональных данных в информационных системах персональных данных».

4.2. Пользователи

Пользователь - работник ООО «Бауцентр Рус», осуществляющий обработку ПДн.

Пользователи назначаются приказом генерального директора ООО «Бауцентр Рус»:

- ❖ «Об утверждении списка лиц, имеющих доступ к персональным данным, постоянных пользователей информационных систем персональных данных, допущенных в помещения, прав доступа к информационным и техническим ресурсам, перечня персональных данных, подлежащих защите».

Пользователь имеет доступ к обработке ПДн, которая включает в себя: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Пользователь ИСПДн обладает следующим уровнем доступа и знаний:

- ✓ обладает всеми необходимыми знаниями для работы с ПДн;
- ✓ имеет личный идентификатор (имя пользователя) и аутентификатор (пароль).

4.3. Требования к пользователям по обеспечению защиты ПДн

Все работники ООО «Бауцентр Рус», являющиеся пользователями ИСПДн, должны четко знать, и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдать принятый режим безопасности ПДн, а также быть ознакомленными с руководящими инструкциями по информационной безопасности ООО «Бауцентр Рус».

При вступлении в должность нового работника, ответственный за организацию обработки персональных данных и выполнение мероприятий по обеспечению безопасности персональных данных в ООО «Бауцентр Рус» (далее – Ответственный за организацию обработки ПДн) обязан ознакомить работника с необходимыми документами, регламентирующими требования по защите ПДн, а также обучить его правилам работы с ПДн в ИСПДн.

Работники ООО «Бауцентр Рус» должны быть ознакомлены с должностными инструкциями, настоящей **Политикой**, Положением об обработке и защите персональных данных ООО «Бауцентр Рус», принятыми процедурами работы с элементами ИСПДн и СЗПДн.

Работники ООО «Бауцентр Рус», использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, возможность их утери, использования третьими лицами.

Работники ООО «Бауцентр Рус» должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Работники ООО «Бауцентр Рус» должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все работники, как пользователи, должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

При работе с ПДн в ИСПДн работники ООО «Бауцентр Рус» обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов автоматизированных рабочих мест (далее – АРМ).

При завершении работы с ПДн работники обязаны защитить АРМ с помощью блокировки (комбинация Ctrl-Alt-Del, далее Блокировка компьютера; комбинация Клавиша Windows+L).

Работники ООО «Бауцентр Рус» должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Работники ООО «Бауцентр Рус» должны быть ознакомлены с дисциплинарными взысканиями при нарушении требований безопасности ПДн в соответствии с действующим федеральным законодательством Российской Федерации в области защиты информации и персональных данных.

Контроль за соблюдением режима безопасности ПДн возложен на Ответственного за организацию обработки ПДн, в соответствии с приказом генерального директора ООО «Бауцентр Рус»:

❖ **«О назначении ответственного за организацию обработки персональных данных, за эксплуатацию объекта информатизации, создании комиссии по проведению обследования и определению уровня защищенности персональных данных при их обработке в информационных системах персональных данных, разработке и внедрении документов по информационной безопасности».**

Работники ООО «Бауцентр Рус» обязаны без промедления сообщать генеральному директору или Ответственному за организацию обработки ПДн обо всех случаях работы ИСПДн, которые могут повлечь за собой угрозу безопасности ПДн.

Работникам ООО «Бауцентр Рус» **ЗАПРЕЩАЕТСЯ**:

- ✓ устанавливать постороннее программное обеспечение,
- ✓ подключать личные мобильные устройства и носители информации, записывать на них защищаемую информацию.

- ✓ разглашать защищаемую информацию, которая стала им известна при работе в информационных системах ООО «Бауцентр Рус» третьим лицам.

4.4. Должностные обязанности пользователей ИСПДн, администратора информационной безопасности

Обязанности пользователей ИСПДн, администратора информационной безопасности описаны в следующих организационно-распорядительных документах:

- ✓ инструкции пользователя информационных систем персональных данных;
- ✓ инструкции по организации режима доступа в помещения;
- ✓ инструкции администратора информационной безопасности;
- ✓ инструкции по организации режима доступа в помещения;
- ✓ инструкции по организации антивирусной защиты;
- ✓ инструкции по организации парольной защиты;
- ✓ инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации;
- ✓ инструкции о порядке планирования и проведения проверок информационной безопасности в информационных системах персональных данных;
- ✓ должностных инструкциях работников ООО «Бауцентр Рус».

5. Ответственность работников ООО «Бауцентр Рус» обрабатывающих ПДн в ИСПДн

ООО «Бауцентр Рус», как Оператор, обязано назначить работника, ответственного за организацию обработки персональных данных и выполнение мероприятий по обеспечению безопасности персональных данных (Ответственный за организацию обработки ПДн).

Ответственный за организацию обработки ПДн в ООО «Бауцентр Рус» получает указания непосредственно от генерального директора ООО «Бауцентр Рус» и подотчетно ему.

Ответственный за организацию обработки ПДн в ООО «Бауцентр Рус», **ОБЯЗАН:**

- ✓ осуществлять внутренний контроль за соблюдением работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- ✓ доводить до сведения работников ООО «Бауцентр Рус» положения: законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных (приказы, инструкции), требования к защите персональных данных;

- ✓ организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных изложена в:

- ✓ Кодексе об административных правонарушениях Российской Федерации – статьи **5.27, 5.39, 13.11-13.14, 19.4-19.7, 19.20, 20.25, 32.2;**
- ✓ Уголовном Кодексе Российской Федерации – статьи **137, 140, 155, 183, 272, 273, 274, 292, 293;**
- ✓ Трудовом Кодексе Российской Федерации – статьи **81, 90, 195, 237, 391.**

Администратор ИБ ООО «Бауцентр Рус» несет ответственность за все действия, совершенные от имени учетных записей или системных учетных записей пользователей, если не доказан факт несанкционированного использования учетных записей.