|  |  |
| --- | --- |
|  |  |
|  |

### КОНЦЕПЦИЯ

**обеспечения безопасности в ООО «\_\_\_\_\_\_\_\_\_\_\_\_\_»**

**Москва, 2023 г.**

**Содержание**

[1. ОБЩАЯ Информация оБ ОБЪЕКТЕ 4](#_Toc152063943)

[1.1. Общие сведения 4](#_Toc152063944)

[1.2. Особенности функционирования Комплексной системы безопасности 4](#_Toc152063945)

[1.3. Факторы, влияющие на обеспечение безопасности Общества 5](#_Toc152063946)

[1.4. Вводимые определения сокращений и терминов 6](#_Toc152063947)

[Таблица 1. Перечень сокращений 6](#_Toc152063948)

[Таблица 2. Перечень терминов 7](#_Toc152063949)

[2. правовые основы обеспечения безопасности 10](#_Toc152063950)

[2.1. Законодательство о безопасности 10](#_Toc152063951)

[2.2. Законодательство об охране правопорядка 11](#_Toc152063952)

[3. ЦЕЛИ И ЗАДАЧИ СИСТЕМЫ БЕЗОПАСНОСТИ 15](#_Toc152063953)

[3.1. Цели системы безопасности 15](#_Toc152063954)

[3.2. Задачи системы безопасности 15](#_Toc152063955)

[4. Угрозы безопасности общества. объекты их воздействия. субъекты реализации 16](#_Toc152063956)

[4.1. Угрозы безопасности Общества 16](#_Toc152063957)

[4.2. Объекты воздействия угрозы 18](#_Toc152063958)

[4.3. Субъекты угроз 18](#_Toc152063959)

[4.4. Критерии последствий реализации угроз 19](#_Toc152063960)

[5. ПРИНЦИПЫ ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ БЕЗОПАСНОСТи 19](#_Toc152063961)

[5.1. Принципы организации системы безопасности 19](#_Toc152063962)

[5.2. Деятельность по обеспечению безопасности 22](#_Toc152063963)

[6. Силы и средства обеспечения безопасности 22](#_Toc152063964)

[6.1. Силы обеспечения безопасности 22](#_Toc152063965)

[6.2. Средства обеспечения безопасности 22](#_Toc152063966)

[6.3. Дополнительные силы и средства обеспечения безопасности 22](#_Toc152063967)

[7. элементы комплексной системы обеспечения безопасности 23](#_Toc152063968)

[7.1. Антитеррористическая защищенность 23](#_Toc152063969)

[7.2. Внутренняя безопасность 24](#_Toc152063970)

[7.3. Экономическая безопасность 25](#_Toc152063971)

[7.4. Информационная безопасность 25](#_Toc152063972)

[7.5. Правовые меры обеспечения безопасности 27](#_Toc152063973)

[7.6. Комплексное обеспечение безопасности территории 27](#_Toc152063974)

[8. подразделение безопасности 30](#_Toc152063975)

[8.1. Основные задачи Подразделения безопасности 30](#_Toc152063976)

[8.2. Задачи Подразделения безопасности, передаваемые на аутсорсинг 31](#_Toc152063977)

[8.3. Структура Подразделения безопасности 33](#_Toc152063978)

[9. Заключительная часть 34](#_Toc152063979)

1. ОБЩАЯ Информация оБ ОБЪЕКТЕ
   1. Общие сведения

ООО «\_\_\_\_\_\_\_\_\_» (далее – Общество) является \_\_\_\_\_\_\_\_\_\_ (указать значимость для региона, района, вклад в городскую бизнес-среду, место на рынке аналогичной деятельности).

Общество - это крупнейший и наиболее известный \_\_\_\_\_\_\_\_\_\_\_\_\_.

Общество оказывает комплекс услуг/ производит/ добывает/ перерабатывает (изменить под свою специфику) по организации \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Общество имеет единую территорию общей площадью - \_\_\_\_\_ га, включая \_\_\_\_\_\_ га промышленной/производственной зоны, на которой расположено \_\_\_\_\_\_\_ объектов недвижимого имущества, из которых:

* \_\_\_ ед. - находится в собственности Общества;
* \_\_\_ ед. - в федеральной собственности;
* \_\_\_ ед. - в собственности города \_\_\_\_\_\_\_\_;
* \_\_\_ ед. - в частной собственности;
* в числе этих объектов \_\_\_ ед. объектов природоохранного значения;
* \_\_\_ ед. – добавить с учетом специфики бизнес-процессов.

Для обеспечения жизнедеятельности на территории, размещена разветвленная сеть инженерной инфраструктуры (водопроводные и электрические сети, насосные станции, трансформаторные подстанции, артезианские скважины и др.) (добавить с учетом специфики бизнес-процессов).

По периметру объекта организованно \_\_\_\_\_\_\_\_ мест для входа на территорию и \_\_\_\_\_\_\_\_\_\_ КПП для въезда-выезда автотранспорта.

* 1. Особенности функционирования Комплексной системы безопасности

Характерными особенностями функционирования Комплексной системы безопасности Общества являются:

* большая площадь комплекса с наличием разнотипных объектов (краткое описание производственных, офисных, транспортных объектов, с т.з. из назначения), обуславливающих разнообразие возможных угроз и опасностей;
* наличие на территории Общества зон и объектов, за которыми затруднен визуальный контроль;
* объекты, потенциально представляющих повышенную опасность (в т.ч. АЗС, газовая котельная, газопровод, оборудование высоковольтного энергоснабжения);
* скопление большого количества автотранспорта одновременно на ограниченном пространстве;
* широкая огласка и общественный резонанс при возникновении любого чрезвычайного происшествия на территории Общества;
* добавить с учетом специфики бизнес-процессов.

Эти особенности повышают вероятность и возможность проведения акций террористического и экстремистского характера.

Для недопущения подобных акций необходимо постоянно разрабатывать и реализовывать мероприятия по совершенствованию Комплексной системы безопасности.

Комплексная система безопасности Общества должна быть, в первую очередь, ориентирована на профилактику и предотвращение наиболее опасных угроз, обеспечивать своевременное принятие решений по предотвращению (недопущению, ликвидации последствий) угроз на основе контроля и наблюдения за территорией, зданиями и строениями, постоянного мониторинга систем жизнеобеспечения, анализа складывающейся обстановки и включать в себя комплексное использование имеющихся технических средстве и привлекаемых сил.

* 1. Факторы, влияющие на обеспечение безопасности Общества

К основным факторам, влияющим на обеспечение безопасности Общества можно отнести:

* повышение градообразующей, экономической, имиджевой, репутационной значимости объекта;
* усиление внимания со стороны правоохранительных и государственных органов;
* сопутствующие диверсифицированные виды деятельности;
* развитие инвестиционной привлекательности объекта.
  + 1. Повышение градообразующей, экономической, имиджевой, репутационной значимости объекта

Общество является градообразующим в связи со значительным \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Имея в штате \_\_\_\_\_\_\_\_\_\_\_\_ человек, Общество способствует \_\_\_\_\_\_\_\_\_\_\_\_, в т.ч. в бюджет региона\_\_\_\_\_\_\_\_\_\_\_\_\_.

Позитивный имидж Обществу обеспечивает его поддержка\_\_\_\_\_\_\_\_\_\_\_\_. Соответственно любые события негативного характера могут иметь не только последствия как для самих сотрудников Общества, так и для \_\_\_\_\_\_\_\_\_\_.

По таким фактам сторонние наблюдатели оценивают социальную стабильность, эффективность мероприятий в области обеспечения безопасности, способность противостоять рискам и угрозам.

Имиджевые и репутационные риски могут иметь серьезные последствия как для всего Общества, так и для его руководителей.

* + 1. Усиление внимания со стороны государственных органов

В соответствии с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Общество является \_\_\_\_\_\_\_\_\_\_\_\_\_.

В ходе модернизации производственных площадей было принято решение о \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. В связи с этим все \_\_\_\_\_\_\_\_\_ работы, вся деятельность, осуществляемая на территории Общества, находятся под пристальным вниманием государственных органов власти, общественности.

* + 1. Перепрофилирование деятельности

В настоящий момент часть объектов Общества передана \_\_\_\_\_\_\_\_\_\_\_\_.

В дальнейшем на территории Общества планируется \_\_\_\_\_\_\_\_\_\_\_\_. На площадях должны быть \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

В перспективе планируется развивать Общество как крупнейший \_\_\_\_\_\_\_\_\_\_ региона.

* + 1. Развитие инвестиционной привлекательности объекта

С \_\_\_\_\_\_\_ года на территории Общества задействовано около \_\_\_\_\_\_\_ человек и более \_\_\_\_\_\_\_\_ тысячи единиц техники.

За это время было построено \_\_\_\_\_\_\_\_\_\_\_ зданий и сооружений, заменено \_\_\_\_\_\_\_\_ тыс. кв. м асфальта, снесено \_\_\_\_\_\_\_\_ временных и незаконных строений, отремонтировано \_\_\_\_\_ км электросетей, приведен в порядок уникальный природный ландшафт на прилегаемой территории.

* 1. Вводимые определения сокращений и терминов

Концепция обеспечения безопасности Общества (далее — Концепция):

* определяет на основе изучения современного состояния безопасности цели, задачи и способы защиты Общества от воздействия рисков, угроз, а также противоправных деяний;
* рассматривает Общество, как объект угроз, противоправных посягательств и иных деяний, содержит описание рисков и их возможных последствий;
* излагает методы и средства выявления, предотвращения, пресечения и минимизации угроз, а также особенности обеспечения безопасности различных видов деятельности;
* излагает основные направления деятельности Подразделения безопасности;
* описывает организационную структуру подразделения безопасности, принципы построения комплексной системы безопасности.

Концепция предназначена для использования в качестве методологической основы при разработке комплекса нормативных правовых, организационных и методических документов, регламентирующих деятельность в области обеспечения безопасности Общества.

Таблица 1. Перечень сокращений

| Сокращение | Расшифровка сокращения |
| --- | --- |
| УК | Управляющая компания |
| Общество | ООО «\_\_\_\_\_\_\_\_\_\_\_\_\_» |
| ДО | Дочернее Общество |
| ПБ | Подразделение безопасности |
| ВНД | Внутренние нормативные документы |
| ПДЗ | Просроченная дебиторская задолженность |
| ЭБ | Экономическая безопасность |
| ВБ | Внутренняя безопасность |
| ИБ | Информационная безопасность |
| СУИБ | Система управления информационной безопасностью |
| ИСПДн | Информационная система персональных данных |

Таблица 2. Перечень терминов

| Наименование термина | Определение термина |
| --- | --- |
| **Безопасность компании** | Состояние защищенности компании от воздействия внутренних и внешних рисков и угроз |
| **Стратегия безопасности** | Общий, недетализированный план деятельности в области обеспечения безопасности, охватывающий длительный период времени |
| **Комплексная система безопасности** | Совокупность организационных, распорядительных, нормативных, технических и административных мероприятий, средств и документов, направленная на всестороннее обеспечение экономической, внутренней, информационной безопасности |
| **Внутренняя безопасность** | Совокупность организационных, административных, информационных, нормативных мер, направленных на предотвращение, нейтрализацию, локализацию угроз в отношении сотрудников Общества, информации, составляющей коммерческую тайну, его материальным и денежным средствам, зданиям и сооружениям, ликвидацию негативных последствий их возникновения. |
| **Экономической безопасность** | Совокупность организационных, административных, информационных, нормативных мер, направленных на предотвращение, нейтрализацию, локализацию угроз финансово-хозяйственной деятельности Общества, его материальным и денежным средствам, зданиям и сооружениям, ликвидацию негативных последствий их возникновения. |
| **Информационная безопасность** | Состояние, обеспечивающее защищенность информации, информационных носителей, ресурсов, каналов, информационных систем от несанкционированного или непреднамеренного изменения или уничтожения информации с одновременным предоставлением к ней своевременного доступа субъектам, обладающим соответствующим допуском, и отказа в таком праве неуполномоченным субъектам. |
| **Безопасность жизнедеятельности** | Состояние защищенности персонала структурных подразделений, дочерних обществ, посетителей, постоянного и выставочного оборудования от рисков и угроз, могущих возникнуть в результате преднамеренных (террористических) действий, техногенных аварий, опасных природных явлений и других опасностей |
| **Угроза безопасности** | Потенциально или реально возможное событие, действие, процесс или явление, которое способно нарушить (повлиять) на финансово-хозяйственную деятельность Общества или привести к остановке его деятельности |
| **Защита безопасности** | Реализация мер правового, нормативного, организационно-технического и специального (детективного, криминалистического и т.д.) характера, направленных на предупреждение, выявление и пресечение противоправных деяний, представляющих угрозу интересам Общества |
| **Антитеррористическая защищенность объектов** | Совокупность мер защиты, направленных на выявление и предотвращение проявления террористических угроз |
| **Терроризм** | Это насилие или угроза его применения в отношении фи­зических лиц или организации, а также уничтожение (повреждение) или угроза уничтожения (повреждения) имущества и других материальных объектов, создающие опасность гибели людей, причинения значительно­го имущественного ущерба либо наступления иных общественно опасных последствий, осуществляемые в целях нарушения общественной безопас­ности, устрашения населения или оказания воздействия на принятие орга­нами власти решений, выгодных террористам, или удовлетворения их не­правомерных имущественных и (или) иных интересов |
| **Объект обеспечения безопасности** | Элемент инфраструктуры Общества, на котором может возникать и развиваться кризисная ситуация, в том числе, здания, павильоны, водо- и газопроводы, а также другие сооружения и участки территории, расположенные в непосредственной близости |
| **Кризисная ситуация** | Ситуация, при которой возникает или реализуется угроза безопасности финансово-хозяйственной и повседневной деятельности Общества |
| **Обеспечение безопасности** | Целенаправленная деятельность по предупреждению, выявлению нестандартных (кризисных) ситуаций, а также адекватному реагированию на них |
| **Правовое обеспечение** | Нормативное закрепление, юридическое регулирование и сопровождение направлений деятельности компании, бизнес-процессов, процедур |
| **Мониторинг безопасности объектов** | Сбор, обработка и анализ информации о состоянии антитеррористического защищенности объектов, безопасности персонала структурных подразделений и дочерних обществ и посетителей, а также - факторов, влияющих на это состояние |
| **Методика обеспечения безопасности** | Взаимосвязанная система научно обоснованных приемов, правил и рекомендаций, применяемых в целях организации и осуществления защиты Общества от противоправных посягательств |
| **Объект противоправного посягательства** | Имущество, финансовые средства, здания и сооружения Общества, приравненные к нему объекты гражданского права вне зависимости от вида и назначения обеспечения, нематериальные активы, руководство и персонал, а также система создания и функционирования Общества, используемые технологии и средства их технического обеспечения |
| **Субъект противоправного посягательства** | Лицо, фактор, обстоятельство, причастное к реализации угроз |
| **Требования безопасности** | Система условий, запретов, ограничений и других обязательных требований, содержащихся в федеральных законах и иных нормативных правовых актах, а также в нормативных технических документах, внутренних (локальных) нормативных актах, соблюдение которых призвано обеспечить безопасность деятельности |
| **Эффективность системы безопасности** | вероятность выполнения системой своей основной целевой функции по обеспечению защиты объекта от угроз, источником которых является посягательство на интересы Общества |

1. правовые основы обеспечения безопасности

Правовые основы безопасности Общества определяют соответствующие положения Конституции Российской Федерации, Закон "О безопасности", федеральные законы и другие нормативные акты.

Правовая защита персонала Общества, его материальных и экономических интересов от посягательств обеспечивается на основе норм Уголовного и Уголовно-процессуального кодексов, законов Российской Федерации о прокуратуре, о федеральной службе безопасности, о милиции, об оперативно-розыскной деятельности, о частной детективной и охранной деятельности, об оружии и др.

Защиту имущественных и иных материальных интересов, деловой репутации Общества призваны обеспечивать также гражданское, гражданско- процессуальное и арбитражное и арбитражно-процессуальное законодательство.

Обеспечение безопасности регулируется законами Российской Федерации: «О коммерческой тайне», «О закупках товаров, работ, услуг отдельными видами юридических лиц», «Об информации, информатизации и защите информации», «О персональных данных», «О противодействии терроризму», «О частной детективной и охранной деятельности в Российской Федерации» и другие.

Успешное и эффективное решение задач обеспечения безопасности достигается формированием системы внутренних нормативных актов, инструкций, положений, правил, регламентов и функциональных обязанностей сотрудников линейных подразделений и служб, в том числе и службы безопасности. Требования по правовому обеспечению безопасности предусматриваются во всех структурно-функциональных правовых документах, начиная с Устава Общества и кончая функциональными обязанностями каждого сотрудника.

* 1. Законодательство о безопасности
     1. Закон РФ «О безопасности» от 28.12.2010 г. № 390-ФЗ

Настоящий Федеральный закон определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством Российской Федерации (далее - безопасность, национальная безопасность), полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области безопасности.

* + 1. Закон РФ «О противодействии терроризму» от 06.03.2006 года N 35-ФЗ

Настоящий Федеральный закон устанавливает основные принципы противодействия терроризму, правовые и организационные основы профилактики терроризма и борьбы с ним, минимизации и (или) ликвидации последствий проявлений терроризма.

Федеральный закон устанавливает основные понятия, принципы и организационные основы противодействия терроризму.

Определено, что антитеррористическая защищенность объекта (территории) это - состояние защищенности здания, строения, сооружения, иного объекта, места массового пребывания людей, препятствующее совершению террористического акта. При этом под местом массового пребывания людей понимается территория общего пользования поселения или городского округа, либо специально отведенная территория за их пределами, либо место общего пользования в здании, строении, сооружении, на ином объекте, на которых при определенных условиях может одновременно находиться более пятидесяти человек.

* 1. Законодательство об охране правопорядка
     1. Закон РФ «О полиции» от 07.02.2011 г. № 169-ФЗ

Исходя из содержания ст. 2, определяет основные направления деятельности для полиции в обеспечении правопорядка:

* защита личности, общества, государства от противоправных посягательств;
* предупреждение и пресечение преступлений и административных правонарушений;
* выявление и раскрытие преступлений, производство дознания по уголовным делам;
* производство по делам об административных правонарушениях, исполнение административных наказаний;
* обеспечение правопорядка в общественных местах;
* охрана имущества и объектов, в том числе на договорной основе.
  + 1. Закон РФ «О частной детективной и охранной деятельности в Российской Федерации»от 11.03*.*1992 г. № 2487-I

Указанный закон позволяет Обществу пользоваться для обеспечения безопасности услугами детективного и охранного характера, в том числе:

* заключить договор с частным детективом;
* заключить договор с охранным предприятием.

В рамках заключенных договоров по запросу Общества могут быть оказаны следующие услуги:

* сбор сведений по гражданским делам на договорной основе с участниками процесса;
* изучение рынка, сбор информации для деловых переговоров, выявление некредитоспособных или ненадежных деловых партнеров;
* установление обстоятельств неправомерного использования в предпринимательской деятельности фирменных знаков и наименований, недобросовестной конкуренции, а также разглашения [сведений](consultantplus://offline/ref=7A451FA9CA1CDD2D1FE506B7572F67D746C8C5C9BC9C0B1E212B679C090988F241FA8F522551C1jBS1L), составляющих коммерческую тайну;
* выяснение биографических и других характеризующих личность данных об отдельных гражданах (с их письменного согласия) при заключении ими трудовых и иных контрактов;
* поиск утраченного гражданами или предприятиями, учреждениями, организациями имущества;
* поиск лица, являющегося должником в соответствии с исполнительным документом, его имущества.

В указанном нормативном акте закреплены основные понятия детективной и охранной деятельности.

* + 1. Закон РФ «О коммерческой тайне» от 29.07.2004 г. № 98-ФЗ

Настоящий Федеральный закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, составляющей секрет производства (ноу-хау).

Положения настоящего Федерального закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

В данном акте закреплены понятия коммерческой тайны (далее – КТ), информации, составляющей КТ, определены, сведения, которые не могут составлять КТ.

В соответствии с требованиями закона меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

* определение перечня информации, составляющей коммерческую тайну;
* ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
* учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
* регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
* нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа "Коммерческая тайна" с указанием обладателя такой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).
  + 1. Закон РФ «О закупках товаров, работ, услуг отдельными видами юридических лиц» от 18.07.2011 года N 223-ФЗ

Целями регулирования настоящего Федерального закона являются обеспечение единства экономического пространства, создание условий для своевременного и полного удовлетворения потребностей юридических лиц, указанных в части ст. 2 настоящего закона (далее - заказчики), в товарах, работах, услугах с необходимыми показателями цены, качества и надежности, эффективное использование денежных средств, расширение возможностей участия юридических и физических лиц в закупке товаров, работ, услуг (далее также - закупка) для нужд заказчиков и стимулирование такого участия, развитие добросовестной конкуренции, обеспечение гласности и прозрачности закупки, предотвращение коррупции и других злоупотреблений.

Нормативный акт определяет:

* правовую основы закупки товаров, работ, услуг;
* принципы и основные положения закупки товаров, работ, услуг;
* информационное обеспечение закупки.
  + 1. Закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 года N 149-ФЗ

Настоящий Федеральный закон регулирует отношения, возникающие при:

* осуществлении права на поиск, получение, передачу, производство и распространение информации;
* применении информационных технологий;
* обеспечении защиты информации.

Федеральный закон устанавливает понятия, принципы правового регулирования отношений в области информации, информационных технологиях, защите информации.

Закона «Об информации, информационных технологиях и о защите информации» предусмотрено, что защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

* обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
* соблюдение конфиденциальности информации ограниченного доступа;
* реализацию права на доступ к информации.

Для обеспечения защиты информации Общество обязано обеспечить:

* предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
* своевременное обнаружение фактов несанкционированного доступа к информации;
* предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
* недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
* возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
* постоянный контроль за обеспечением уровня защищенности информации.

* + 1. Закон РФ «О персональных данных» от 27.07.2006 г. № 152-ФЗ.

Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, иными муниципальными органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

Федеральный закон устанавливает понятия в области персональных данных, принципы и условия их обработки, обеспечение конфиденциальности.

Обработка персональных данных может осуществляться только с письменного согласия субъекта персональных данных, которое должно включать в себя, в частности:

* фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
* фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
* наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
* цель обработки персональных данных;
* перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
* наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
* перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
* срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
* подпись субъекта персональных данных.

1. ЦЕЛИ И ЗАДАЧИ СИСТЕМЫ БЕЗОПАСНОСТИ
   1. Цели системы безопасности

Главной целью системы безопасности является обеспечение устойчивого функционирования Общества и предотвращение угроз его безопасности, защита законных интересов от противоправных посягательств, охрана жизни и здоровья персонала, недопущения хищения финансовых и материально-технических средств, уничтожения имущества и ценностей, разглашения, утраты, утечки, искажения и уничтожения информации, составляющей коммерческую тайну, нарушения работы технических средств, обеспечения производственной деятельности, включая и средства информатизации.

Другими целями Концепции являются:

* формирование целостного представления о системе безопасности Общества и взаимоувязка различных элементов этой системы, определение путей реализации мероприятий, обеспечивающих необходимый уровень надежной защищенности объектов;
* повышение имиджа Общества и роста прибыли за счет обеспечения высокого качества предоставляемых услуг и гарантий безопасности клиентов и посетителей.
  1. Задачи системы безопасности

Задачами системы безопасности являются:

* прогнозирование и своевременное выявление и устранение угроз безопасности персоналу и имуществу Общества, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развитию;
* комплексное воздействие на потенциальные и реальные угрозы;
* отнесение информации к категории ограниченного доступа (служебной, коммерческой тайнам, иной конфиденциальной информации, подлежащей защите от неправомерного использования), а других ресурсов - к различным уровням уязвимости (опасности) и подлежащих сохранению;
* создание механизма и условий оперативного реагирования на угрозы безопасности и проявление негативных тенденций в функционировании Общества;
* эффективное пресечение угроз персоналу и посягательств на имущество, ресурсы на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;
* создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерным действиям физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности на достижение стратегических целей Общества;
* обеспечение устойчивого функционирования его структурных подразделений, дочерних обществ и предотвращение угроз безопасности жизнедеятельности Общества;
* повышение конкурентоспособности Общества;
* ориентация на мировые стандарты и лидерство в разработке и освоении (использовании) новых технологий обеспечения безопасности.

1. Угрозы безопасности общества. объекты их воздействия. субъекты реализации

Для Общества, как одной из специфических территорий, наиболее характерны следующие угрозу:

* террористическая;
* техногенная;
* природная;
* уничтожение, порча имущества, зданий, сооружений;
* хищение товарно-материальных ценностей.
  1. Угрозы безопасности Общества
     1. Террористические угрозы

**Терроризм** — это насилие или угроза его применения в отношении фи­зических лиц или организации, а также уничтожение (повреждение) или угроза уничтожения (повреждения) имущества и других материальных объектов, создающие опасность гибели людей, причинения значительно­го имущественного ущерба либо наступления иных общественно опасных последствий, осуществляемые в целях нарушения общественной безопас­ности, устрашения населения или оказания воздействия на принятие орга­нами власти решений, выгодных террористам, или удовлетворения их не­правомерных имущественных и (или) иных интересов.

К основным **угрозам террористического характера** относятся:

* проникновение террористической группы (групп) на территорию Общества с целью захвата заложников, уничтожения людей в местах их массового нахождения;
* подрыв взрывных устройств (ВУ) на территории Общества во время нахождения там больших групп людей или важных государственных и общественных деятелей;
* проникновение террориста-одиночки на территорию Общества или в его здания и сооружения с целью уничтожения посетителей и персонала путем подрыва размещенных под одеждой, в ручной клади, в автомашине взрывных устройств, или с использованием огнестрельного (холодного) оружия и специальных средств;
* применение отравляющих или радиоактивных веществ в местах массового пребывания людей на территории В Общества;
* радиационное заражение местности;
* использование систем приточной вентиляции в помещениях для распыления зловонных, отравляющих и радиоактивных веществ во время проведения массовых или общественно значимых мероприятий;
* поджог зданий и сооружений;
* вывод из строя оборудования систем обеспечения безопасности зданий и сооружений, а также систем инженерного оборудования и коммуникаций;
* отравление(заражение) систем водоснабжения, продуктов питания, водоемов;
* искусственное распространение возбудителей инфекционных болезней.
  + 1. Угрозы техногенного характера

Техногенная угроза - возможное вредное физическое, химическое и механическое воздействие на население и среду обитания в результате производственной деятельности человека, а также аварий (катастроф) на предприятиях.

Наличие значительного количества объектов техносферы, изношенность инженерных сооружений, коммуникаций и зданий на территории Общества несут в себе высокую вероятность наступления риска техногенных аварий и катастроф, к которым можно отнести:

* аварии оборудования (аттракционов, водо-, газо-, электроснабжения и пр.) в местах значительного количества посетителей;
* затопление помещений, зданий, территории;
* короткое замыкание электропроводки;
* пожары в местах концентрированного нахождения посетителей.

В результате реализации угрозы техногенного характера возникает техногенная чрезвычайная ситуация - состояние, при котором в результате возникновения источника техногенной чрезвычайной ситуации на объекте, определенной территории нарушаются нормальные условия жизни и деятельности людей, возникает угроза их жизни и здоровью, наносится ущерб имуществу населения, народному хозяйству и окружающей природной среде.

* + 1. Природные угрозы

Природные угрозы возникают, как правило, при полном отсутствии человеческого фактора, отличаются своей разрушительностью, непредсказуемостью и значимой величиной негативных последствий как экономического, так и социального характера.

Природная чрезвычайная ситуация – обстановка на определенной территории, сложившаяся в результате возникновения источника природной чрезвычайной ситуации, который может повлечь или повлек за собой человеческие жертвы, ущерб здоровью людей и (или) окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности людей.

К основным природным угрозам относятся вероятные затяжные дожди, ураганы, обледенения дорог, сильные снегопады, землетрясения.

* + 1. Экономические угрозы

В реализации экономических угроз большое значение играет человеческий фактор, основанный на желании улучшить свое материальное положение, занять более выгодные позиции по сравнению с конкурентами, создать преференции для своего бизнеса.

К основным экономическим угрозам Общества можно отнести:

* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
  1. Объекты воздействия угрозы

Понятие Общества как объекта воздействия угроз тесно связано с понятиями «деятельность Общества», «средства деятельности Общества» и «процесс деятельности Общества». Средства деятельности Общества (включая неимущественные права и нематериальные блага) являются составной частью имущества Общества.

Все виды деятельности, обеспечивающей функционирование Общества и создание соответствующих условий для его функционирования, охватываются понятием «инфраструктура Общества».

Имущество и инфраструктура Общества являются ведущими объектами воздействия угроз.

К объектам воздействия угроз относятся:

* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
  1. Субъекты угроз

Учитывая специфику деятельности Общества, его производственных процессов, состояние зданий и сооружений, ряд объектов угроз может стать субъектами их реализации.

В связи с этим субъектами угроз выступают:

* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
  1. Критерии последствий реализации угроз

Противоправные посягательства на безопасность Общества классифицируются по следующим основаниям.

Непосредственный объект защиты:

* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Виды деятельности, в процессе которых совершено посягательство:

* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Степень тяжести ущерба, причиненного реализовавшимися угрозами:

* восполнимый (незначительный) ущерб — потери имущества и элементов инфраструктуры, которые можно восполнить за счет собственных средств без угрозы своему существованию и без перевода Общества во внештатный режим работы;
* условно восполнимый ущерб — потери имущества, создающие угрозу существованию Общества, которые оно не может устранить без привлечения внешних средств. Внешними инструментами восполнения потерь в данных случаях могут служить заемные финансовые средства, привлеченный для восстановления управления новый персонал (вплоть до введения внешнего управления), приобретение новых технических средств обеспечения безопасности. Для возмещения условно восполнимых потерь Общество вынуждено переходить на внештатный режим работы;
* невосполнимый (катастрофический, значительный, существенный) ущерб — потери имущества и инфраструктуры Общества, возместить которые не представляется возможным, а его причинение влечет ликвидацию или реорганизацию.

1. ПРИНЦИПЫ ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ БЕЗОПАСНОСТи
   1. Принципы организации системы безопасности

Основными принципами обеспечения безопасности являются:

* комплексность;
* своевременность;
* непрерывность;
* активность;
* законность;
* обоснованность;
* экономическая целесообразность и сопоставимость;
* плановость;
* специализация;
* взаимодействие и координация;
* совершенствование;
* централизация управления;
* системность.

Комплексность заключается в:

* обеспечении безопасности персонала, материальных и финансовых ресурсов от возможных угроз всеми доступными законными средствами, методами и мероприятиями;
* обеспечении безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их обработки (преобразования) и использования, во всех режимах функционирования;
* способности системы к развитию и совершенствованию в соответствии с изменениями условий функционирования Общества.

Комплексность достигается:

* обеспечением соответствующего режима и охраны;
* организацией специального делопроизводства с ориентацией на защиту конфиденциальной информации и персональных данных;
* мероприятиями по подбору и расстановке кадров;
* широким использованием технических средств безопасности и защиты информации;
* информационно-аналитической и детективной деятельностью.

Комплексность реализуется совокупностью правовых, организационных и инженерно-технических мероприятий.

**Своевременность** – носит упреждающий характер мер обеспечения безопасности.

Своевременность предполагает постановку задач по комплексной безопасности на ранних стадиях разработки системы безопасности на основе анализа и прогнозирование финансовой обстановки, угроз безопасности, а также разработку эффективных мер предупреждения посягательств на законные интересы.

**Непрерывность** – постоянный характер реализации мер обеспечения безопасности, комбинированное применение соответствующих технических средств и физической охраны.

**Активность.** Защищать интересы Общества необходимо с достаточной степенью настойчивости, широко используя маневр силами и средствами обеспечения безопасности и нестандартные меры защиты.

**Законность.** Предполагает разработку системы безопасности на основе федерального законодательства в области информатизации и защиты информации, частной охранной деятельности и других нормативных актов по безопасности, утвержденных органами государственного управления в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений.

**Обоснованность.** Используемые возможности и средства защиты должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и соответствовать установленным требованиям и нормам.

**Экономическая целесообразность и сопоставимость** возможного ущерба и затрат на обеспечение безопасности (критерий "эффективность - стоимость"). Во всех случаях стоимость системы безопасности должна быть меньше размера возможного ущерба от любых видов риска.

**Плановость.** Деятельность по обеспечению безопасности строится на основе комплексной программы обеспечения безопасности, подпрограмм обеспечения безопасности по основным её видам (экономическая, научно-техническая, экологическая, технологическая и т.д.) и разрабатываемых для их исполнения планов работы подразделений Общества и отдельных сотрудников

**Специализация.** Предполагается привлечение к разработке и внедрению мер и средств защиты специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Эксплуатация технических средств и реализация мер безопасности должны осуществляться профессионально подготовленными специалистами службы безопасности Общества, его функциональных и обслуживающих подразделений.

**Взаимодействие и координация.** Означает осуществление мер обеспечения безопасности на основе четкой взаимосвязи соответствующих подразделений и служб, сторонних специализированных организаций в этой области, координации их усилий для достижения поставленных целей, а также сотрудничества с заинтересованными объединениями и взаимодействия с органами государственного управления и правоохранительными органами.

**Совершенствование.** Предусматривает совершенствование мер и средств защиты на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах разведки и промышленного шпионажа, нормативно-технических требований, достигнутого отечественного и зарубежного опыта.

**Централизация управления.** Предполагает самостоятельное функционирование системы безопасности по единым правовым, организационным, функциональным и методологическим принципам и централизованным управлением деятельностью системы безопасности.

**Системность.** Учет всех факторов, оказывающих влияние на безопасность Общества, включение в деятельность по её обеспечению всех сотрудников структурных подразделений Общества и дочерних обществ, использование в этой деятельности всех сил и средств.

* 1. Деятельность по обеспечению безопасности

Деятельность по обеспечению безопасности включает в себя:

* прогнозирование, выявление, анализ и оценку угроз безопасности;
* определение основных направлений и стратегическое планирование в области обеспечения безопасности;
* правовое регулирование в области обеспечения безопасности;
* разработку и применение комплекса оперативных и долговременных мер по выявлению, предупреждению и устранению угроз безопасности, локализации и нейтрализации последствий их проявления;
* применение специальных экономических мер в целях обеспечения безопасности;
* осуществление других мероприятий в области обеспечения безопасности в соответствии с законодательством Российской Федерации.

1. Силы и средства обеспечения безопасности

Силы комплексной системы безопасности Общества включают штатный состав службы безопасности и иных лиц, привлекаемых для решения отдельных задач защиты, охраны, предупреждения преступных посягательств и сыска.

* 1. Силы обеспечения безопасности

К силам обеспечения безопасности относятся:

* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
  1. Средства обеспечения безопасности

К средствам обеспечения безопасности относятся:

* Инженерно-технический центр мониторинга (сбор и обработка информации);
* системы видеонаблюдения, сигнализации, управления доступом, проездом;
* специальные средства, использующиеся в частной детективной и охранной деятельности в целях обеспечения индивидуальной защиты и пресечения противоправных посягательств;
* спецавтотранспорт, использующийся для своевременного реагирования по возникшим инцидентам, проведению операций по инкассации;
* система связи и система передачи данных;
* средства защиты информации, включая средства криптографической защиты.
  1. Дополнительные силы и средства обеспечения безопасности

Для обеспечения безопасности мероприятий на территории Общества в соответствии с \_\_\_\_\_\_\_\_\_\_\_\_, решениями других государственных структур, а также в зависимости от \_\_\_\_\_\_\_\_\_\_\_\_ или с участием \_\_\_\_\_\_\_\_\_\_\_\_, дополнительно привлекаются силы и средства \_\_\_\_\_\_\_\_\_\_\_\_.

1. элементы комплексной системы обеспечения безопасности

Комплексная система обеспечения безопасности включает в себя следующие элементы:

* антитеррористическая защищенность;
* внутренняя безопасность;
* экономическая безопасность;
* информационная безопасность;
* правовые меры обеспечения безопасности;
  1. Антитеррористическая защищенность

Антитеррористическая защищенность:

* совокупность мер, обеспечивающих защищенность зданий, павильонов и других объектов от воздействия террористических угроз;
* антитеррористическая защищенность объекта (территории) - состояние защищенности здания, строения, сооружения, иного объекта, места массового пребывания людей, препятствующее совершению террористического акта[[1]](#footnote-1).

Требования по антитеррористической защищенности объекта должны бать направлены на:

* воспрепятствование неправомерному проникновению на объект (территорию);
* выявление потенциальных нарушителей установленного на объекте (территории) режима и (или) признаков подготовки или совершения террористического акта;
* пресечение попыток совершения террористического акта на объекте (территории);
* минимизацию возможных последствий и ликвидацию угрозы террористического акта на объекте (территории).

Для реализации требований антитеррористической защищенности в Обществе разрабатываются паспорта безопасности, в которых определяются:

* общие сведения об объекте (о территории) (основной вид деятельности, категория, наименование вышестоящей организации по принадлежности и общая площадь);
* общие сведения о работниках и (или) об арендаторах объекта (территории);
* сведения о потенциально опасных участках и (или) критических элементах объекта (территории);
* возможные последствия в результате совершения террористического акта на объекте (территории);
* оценку социально-экономических последствий террористического акта на объекте (территории) (людские потери, нарушения инфраструктуры и экономический ущерб);
* силы и средства, привлекаемые для обеспечения антитеррористической защищенности объекта (территории);
* меры по инженерно-технической, физической защите и пожарной безопасности объекта (территории);
* выводы и рекомендации;
* дополнительная информация с учетом особенностей объекта (территории)[[2]](#footnote-2).
  1. Внутренняя безопасность

Внутренняя безопасность - совокупность организационных, административных, информационных, нормативных мер, направленных на предотвращение, нейтрализацию, локализацию угроз в отношении сотрудников Общества, информации, составляющей коммерческую тайну, его материальным и денежным средствам, зданиям и сооружениям, ликвидацию негативных последствий их возникновения.

* + 1. Основные направления внутренней безопасности:
* изучение кандидатов при приеме на работу;
* проведение внутренних служебных расследований;
* контроль обеспечения режима коммерческой тайны;
* участие в реализации внутриобъектового и пропускного режимов;
* взаимодействие с правоохранительными органами;
* участие в аттестации сотрудников;
* предупреждение фактов мошенничества со стороны сотрудников.
  + 1. Инструменты обеспечения внутренней безопасности

Для реализации основных направлений экономической безопасности могут использоваться:

* информационные порталы органов государственной власти;
* базы консалтинговых компаний;
* легальные ресурсы Интернет;
* внутренние стандарты Общества;
* локальные нормативные акты;
* специалисты консалтинговых компаний.
  1. Экономическая безопасность

Экономической безопасность - совокупность организационных, административных, информационных, нормативных мер, направленных на предотвращение, нейтрализацию, локализацию угроз финансово-хозяйственной деятельности Общества, его материальным и денежным средствам, зданиям и сооружениям, ликвидацию негативных последствий их возникновения.

* + 1. Основные направления экономической безопасности

Основные направления экономической безопасности являются:

* изучение контрагентов при проведении закупочных процедур, установлении договорных отношений, возврату дебиторской задолженности;
* минимизация рисков при закупочных процедурах;
* выявление и мониторинг аффилированности сотрудников Общества с контрагентами;
* мониторинг изменений существенной информации о контрагенте;
* изучение адресов нахождения и регистрации контрагента;
* изучение учредителей, руководителей контрагента;
* установление аффилированности контрагента, его руководителей, учредителей с ликвидированными компания.
  + 1. Инструменты обеспечения экономической безопасности

Для реализации основных направлений экономической безопасности могут использоваться:

* информационные порталы органов государственной власти;
* базы консалтинговых компаний;
* легальные ресурсы Интернет;
* внутренние стандарты Общества;
* локальные нормативные акты;
* специалисты консалтинговых компаний.
  1. Информационная безопасность

Информационная безопасность- состояние, обеспечивающее защищенность информации, информационных носителей, ресурсов, каналов, информационных систем от несанкционированного или непреднамеренного изменения или уничтожения информации с одновременным предоставлением к ней своевременного доступа субъектам, обладающим соответствующим допуском, и отказа в таком праве неуполномоченным субъектам.

Информационные ресурсы–любая зафиксированная ка каком-либо носителе информация и обеспечивающие ее обработку информационные технологии.

* + 1. Цели обеспечения информационной безопасности

Общество считает свои информационные ресурсы существенными активами. Конфиденциальность, целостность и доступность информационных ресурсов Общества способствуют обеспечению конкурентоспособности, ликвидности и доходности, соответствию законодательству Российской Федерации и улучшению деловой репутации.

Общество намерено применять процессный подход к управлению рисками информационной безопасности. Для этого планируется создавать комплексную систему управления информационной безопасностью и управлять ее жизненным циклом во времени.

* + 1. Основные направления деятельности в области информационной безопасности:

Создание и поддержание во времени комплексной системы управления информационной безопасностью (далее – СУИБ):

* разработка Концепции построения СУИБ (определение ее целевых архитектуры, жизненного цикла и иерархии механизмов снижения рисков ИБ);
* моделирование угроз и возможных нарушителей ИБ;
* выбор необходимых к применению механизмов нейтрализации угроз ИБ (организационные документы[[3]](#footnote-3), программные и технические средства);
* внедрение и поддержание во времени режима коммерческой тайны и механизмов нейтрализации угроз ИБ;
* периодическая оценка соответствия текущего состояния СУИБ целевому состоянию, контроль за соблюдением требований ИБ, мониторинг механизмов снижения рисков ИБ;
* предотвращение, мониторинг и расследование инцидентов ИБ;
* периодический пересмотр в связи с изменениями внутренних или внешних факторов элементов СУИБ.

Обеспечение соответствия бизнес-процессов ОБЩЕСТВО, связанных с обработкой персональных данных, положениям Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных» (далее – «152-ФЗ») и Постановлению Правительства № 687 РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (далее – «687-ПП») во времени:

* периодическая оценка соответствия состояния бизнес-процессов Общества, связанных с обработкой персональных данных, положениям 152-ФЗ и 687-ППа
* реализация планов мероприятий по принятию мер, необходимых для выполнения требований 152-ФЗ и 687-ПП;
* моделирование угроз персональным данным при их обработке в информационных системах персональных данных (далее – ИСПДн);
* проведение полного комплекса работ по проектированию и внедрению систем защиты ИСПДн;
* [обеспечение установленных законодательством Российской Федерации процессов взаимодействия с субъектами персональных данных, с уполномоченным органом по защите прав субъектов персональных данных, с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим технической защиты информации.](#_Toc273647063)
  + 1. Инструменты реализации основных направлений в области информационной безопасности

Для реализации основных направлений в области информационной безопасности могут использоваться:

* информационные порталы органов государственной власти;
* специалисты консалтинговых компаний;
* имеющиеся в Обществе программные и технические средства обеспечения ИБ;
* приобретаемые программные и технические средства обеспечения ИБ.
  1. Правовые меры обеспечения безопасности

Правовое обеспечение – это нормативное закрепление, юридическое регулирование и сопровождение направлений деятельности компании, бизнес-процессов, процедур.

* + 1. Инструменты правового обеспечения безопасности

Правовые меры обеспечения безопасности включают:

* формирование и актуализация базы локальных нормативных актов, регламентирующих деятельность в области обеспечения безопасности;
* включение в договоры, заключаемые с арендаторами, обязательств сторон по обеспечению безопасности;
* формирование инструкций, алгоритмов совместных действий с организациями, органами, участвующими в обеспечении безопасности.
  + 1. Инструменты правового обеспечения безопасности

К нормативным документам правового обеспечения можно отнести:

* Кодекс;
* Положение;
* Инструкция;
* Регламент;
* Стандарт.
  1. Комплексное обеспечение безопасности территории

Комплексная обеспечение безопасности территории включает в себя следующие элементы:

* обеспечение контроля доступа;
* мониторинг обстановки на территории;
* организация маршрутов движения (эвакуации) автотранспорта и посетителей;
* организационные меры обеспечения безопасности;
* техническое обеспечение;
* система охраны объектов.
  + 1. Обеспечение контроля доступа

Мероприятия по обеспечению пропускного режима включают в себя контроль:

* въезда/выезда транспортных средств;
* перемещения транспортных средств по территории;
* прохода посетителей на территорию;
* проход сотрудников Общества в здания и помещения.

Обеспечение въезда/выезда, доступа на территорию включает в себя:

* контроль въезда/выезда транспортных средств на территорию и с территории;
* осмотр транспортных средств на предмет выявления оружия, химически-, биологически-, ядерно- и радиационно- опасных материалов, взрывных устройств, наркотиков и т.д.;
* радиационный контроль въезжающих транспортных средств;
* ограничение проезда транспортных средств к служебным объектам;
* введение временных ограничительных мер на передвижение транспортных средств;
* регулирование въезда/выезда и передвижения транспортных средств путем введения пропускной системы с использованием стандартных форм пропусков и электронных карточек.
  + 1. Мониторинг обстановки на территории

Мониторинг обстановки на территории включает:

* автоматический мониторинг функционирования инженерно-технических систем с целью обнаружения отклонений значимых параметров, режимов работы, состояния и функционирования инженерно-технических систем жизнеобеспечения;
* выявление очагов возгораний;
* применение средств автоматического пожаротушения;
* сбор, обработка и анализ поступающей информации о текущей обстановке с использованием систем видеонаблюдения, экстренного вызова, охранных и пожарных датчики, диспетчерская связь, средств экстренной связи с посетителями и т.д.);
* контроль общественного порядка с использованием патрулей (мобильных групп охраны), группы быстрого реагирования ЧОПа, дежурными администраторами по территории;
* наблюдение за лицами, транспортными средствами, сопровождение с использованием технических средств;
* формирование банка данных по правонарушителям, транспортным средствам и их владельцам, допустивших нарушения общественного порядка, пропускного реи внутриобъектового режимов;
* определение мест возможной закладки взрывных устройств и регулярный их осмотр;
* осуществление радиационного контроля территории.
  + 1. Организация маршрутов движения (эвакуации) автотранспорта и посетителей:
* определение маршрутов движения (эвакуации) транспортных средств;
* определение мест стоянки транспортных средств;
* разделение маршрутов движения (эвакуации) транспорта и массового пребывания или движения людей;
* организация безопасного движения транспортных средств;
* применение ограничивающих инженерно-технических средств для упорядочения движения транспорта и посетителей;
* формирование планов передвижения транспортных средств, эвакуации посетителей при чрезвычайных ситуациях.
  + 1. Организационные меры обеспечения безопасности

Организационные меры обеспечения безопасности включают в себя:

* организация работы инженерно-технического центра мониторинга и обслуживающего персонала;
* порядок выявления и задержания (блокирования) нарушителей;
* контроль состояния и работоспособности средств и систем обеспечения безопасности;
* управление устройствами технических систем обеспечения безопасности и инженерных систем;
* взаимодействие с экстренными службами и органами обеспечения безопасности на районном, окружном и городском уровнях;
* защита информации, составляющей коммерческую тайну;
* постоянный радиационный контроль территории;
* порядок действий при обнаружении радиационного заражения;
* объективный контроль действий дежурных администраторов и персонала службы эксплуатации;
* оповещение сотрудников о возникновении чрезвычайной ситуации и проведение безопасной, беспрепятственной и своевременной эвакуации людей из зданий и сооружений, с территории;
* обучение на постоянной основе персонала структурных подразделений и дочерних обществ действиям в условиях чрезвычайных ситуаций;
* проведение учебных мероприятий по действиям в чрезвычайных ситуациях с привлечением сотрудников Общества, правоохранительных органов, ЧОПа.
  + 1. Техническое обеспечение

Техническое обеспечение территории состоит из:

* оборудования пунктов пропуска специальными средствами досмотра, приборами радиационного контроля;
* оснащения зданий, служебных помещений, сооружений системами охранно-пожарной сигнализации, кнопками тревожной сигнализации и системами контроля доступа, в соответствии с требованиями руководящих документов;
* оснащение сотрудников Подразделения безопасности Общества, иного персонала мобильными системами тревожной сигнализации, работающими по радиоканалу (радиокнопками или радиобрелками);
* создание инженерно-технического центра мониторинга.
  + 1. Система охраны объектов

Система охраны объектов должна предусматривать:

* систему инженерно-технических и организационных мер охраны;
* систему регулирования доступа;
* систему мер (режима) сохранности и контроль вероятных каналов утечки информации;
* многорубежность построения охраны (территории, здания, помещения) по нарастающей;
* определение порядка выдачи разрешений и оформление документов для входа (въезда) на объект;
* определение объемов контрольно-пропускных функций на каждом проходном и проездном пункте;

1. подразделение безопасности

Обеспечение безопасности Общества относится к компетенции Подразделения безопасности.

Функционально и административно Подразделение безопасности подчиняется \_\_\_\_\_\_\_\_\_.

* 1. Основные задачи Подразделения безопасности

К основным задачам Подразделения безопасности относятся:

* выявление причин и предупреждение возникновения рисков и угроз;
* разработка и реализация превентивных мероприятий по предупреждению рисков и угроз;
* обеспечение комплексного подхода в обеспечении безопасности с использованием технических средств и физической охраны;
* мониторинг антитеррористической защищенности объекта;
* эксплуатация, ремонт и обслуживание технических систем безопасности;
* организация взаимодействия, координация деятельности основными и вспомогательными силами и средства обеспечения безопасности;
* руководство мероприятиями по обеспечению экономической, внутренней и информационной безопасности.
  1. Задачи Подразделения безопасности, передаваемые на аутсорсинг

В целях повышения эффективности деятельности Подразделения безопасности, зачади обеспечения безопасности, по которым могут наступить последствия с незначительным финансовым ущербом, а риски существенно не повлияют на финансово-хозяйственную деятельность, целесообразно передать на аутсорсинг.

Услуги, передаваемые на аутсорсинг:

* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
  + 1. Экономическая безопасность

К направлениям экономической безопасности относятся:

* проведение внутренних (корпоративных) расследований по фактам мошенничества, хищений, злоупотреблений сотрудниками Общества;
* изучение деловых партнеров:
* подтверждение регистрационных данных и сбор информации о деятельности компании;
* информация об учредителях: юридических или физических лицах;
* выявление аффилированности учредителей и руководителей компаний с фирмами, имеющими признаки финансовой несостоятельности, «однодневками»;
* изучение адресов нахождения и регистрации контрагента, партнера;
* обеспечение порядка досудебного урегулирования споров и конфликтных ситуаций;
* установление обстоятельств неправомерного использования в предпринимательской деятельности фирменных знаков и наименований;
* мониторинг изменений в существенной информации о контрагенте;
* выявление аффилированности между контрагентами и Сотрудниками Общества при прохождении закупочных процедур.
  + 1. Информационная безопасность

К направлениям информационной безопасности относятся:

* созданию комплексной системы управления информационной безопасностью (далее – СУИБ):
* разработка Концепции построения СУИБ с описанием ее архитектуры, жизненного цикла и иерархии механизмов снижения рисков ИБ;
* разработка планов мероприятий по достижению целевой архитектуры СУИБ;
* разработка модели нарушителя и модели угроз ИБ;
* выбор необходимых к применению механизмов нейтрализации угроз ИБ (нормативно-методические документы[[4]](#footnote-4), программные и технические средства);
* периодическая оценка соответствия текущего состояния СУИБ целевому состоянию, контроль за соблюдением требований ИБ;
* проведение расследований инцидентов ИБ;
* приведение бизнес-процессов, связанных с обработкой персональных данных, в соответствие положениям Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных» (далее – «152-ФЗ»), Постановлению Правительства № 687 РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (далее – «687-ПП»), а также по поддержанию указанного состояния во времени:
* периодическая оценка соответствия состояния бизнес-процессов, связанных с обработкой персональных данных, положениям 152-ФЗ и 687-ПП;
* разработка с учетом специфики хозяйственной деятельности Заказчика планов мероприятий по принятию мер, необходимых для выполнения требований 152-ФЗ и 687-ПП;
* обследование имеющихся информационных систем персональных данных (далее – ИСПДн) и систем их защиты;
* разработка частных моделей угроз ИСПДн;
* определение в соответствии с подзаконными актами уровней защищенности персональных данных при их обработке в ИСПДн;
* разработка технических заданий на создание систем защиты ИСПДн;
* проектирование систем защиты ИСПДн;
* разработка и внесение изменений во внутренние нормативные акты, регламентирующие вопросы, связанные с обработкой персональных данных;
* организация взаимодействия между субъектами персональных данных, с уполномоченным органом по защите прав субъектов персональных данных, с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим технической защиты информации.
  + 1. Кадровая безопасность

К направлениям кадровой безопасности относятся:

* изучение кандидатов при приеме на работу (выявление биографических и других характеризующих личность данных);
* выработка рекомендаций о целесообразности проведения повторных (периодических) проверок для определенных категорий сотрудников в зависимости от занимаемых должностей;
* участие в мероприятиях по аттестации сотрудников Общества;
* выработка рекомендаций по совершенствованию системы кадровой безопасности;
* определение индивидуально-психологических особенностей личности кандидата методом удаленного и автоматизированного (aport-k.ru) психологического тестирования;
* проведение специального психофизиологического исследования (полиграф);
* проведение интервью (собеседований) с сотрудниками Общества и кандидатами на работу, претендующих на замещение руководящих позиций, а также увольняемых при увольнении
* выявление и мониторинг аффилированности сотрудников с потенциальными партнерами Общества.
  + 1. Внутренняя безопасность

К направлениям внутренней безопасности относятся:

* подготовка и проведение переговоров с использованием технических средств;
* организация и участие в проведении служебных разбирательств;
* проведение интервью (собеседований) с сотрудниками, причастных к негативному событию, факту разбирательства;
* сбор доказательной базы о причастности лиц к мошенничеству, краже средств, увода активов и пр.;
* использование полиграфа при проведении служебного расследования, разбирательства;
* проведение технических мероприятий для внутренних расследований;
* сопровождение поиска похищенного имущества;
* контроль конфиденциального делопроизводства;
* разработка и реализация системы мер, регламентирующий порядок использования сведений, составляющих коммерческую тайну
* контроль соблюдения требований режима коммерческой тайны.
  1. Структура Подразделения безопасности

Организационно структура Подразделения безопасности состоит из \_\_\_\_\_\_\_\_\_\_\_\_\_:

* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

1. Заключительная часть

Комплексная система безопасности Общества, в первую очередь с использованием своих сил, средств и возможностей, ориентирована на обеспечение антитеррористической защищенности Общества, внутриобъектового и пропускного режимов, с использованием привлеченных возможностей (ЧОП, консалтинговые компании, правоохранительные органы) профилактику и предотвращение менее опасных рисков и угроз.

Основной целью мероприятий является:

* мониторинг и локализация признаков рисков и угроз;
* анализ поступающей информации по обстановке, состоянию технических средств охраны, возможных инцидентах;
* реагирование и пресечение действий нарушителей, а также минимизация возможных негативных последствий реализации рисков и угроз.

1. Федеральный Закон Российская Федерация № 35-ФЗ от 06.03.2006 г. «О противодействии терроризму» [↑](#footnote-ref-1)
2. Постановление Правительства Российской Федерации N 1244 от 25.12.2013 г. «Об антитеррористической защищенности объектов (территорий) [↑](#footnote-ref-2)
3. Регламентирующие порядок доступа пользователей к информационным ресурсам, в том числе, таким, как Интернет, корпоративная электронная почта, системы хранения данных, ресурсы ERP-системы и т.д., вопросы, связанные с сетевой безопасностью, антивирусной защитой, управлением инцидентами ИБ, аудитом состояния ИБ. [↑](#footnote-ref-3)
4. Регламентирующие порядок доступа пользователей к информационным ресурсам, в том числе, таким, как Интернет, корпоративная электронная почта, системы хранения данных, ресурсы ERP-системы и т.д., вопросы, связанные с сетевой безопасностью, антивирусной защитой, управлением инцидентами ИБ, аудитом состояния ИБ и т.д. [↑](#footnote-ref-4)