**Приложение 6**

[**1. ВВОДНЫЕ ПОЛОЖЕНИЯ 3**](#_Toc148704087)

[**1.1. ВВЕДЕНИЕ 3**](#_Toc148704088)

[**1.2. ЦЕЛИ 3**](#_Toc148704089)

[**1.3. ЗАДАЧИ 3**](#_Toc148704090)

[**1.4. ОБЛАСТЬ ДЕЙСТВИЯ 4**](#_Toc148704091)

[**2. ОБЩИЕ ПОЛОЖЕНИЯ 5**](#_Toc148704092)

[**3. ОБЪЕКТЫ ЗАЩИТЫ, ИНФОРМАЦИОННЫЕ АКТИВЫ 6**](#_Toc148704093)

[**4. ПРИНЦИПЫ, ПРАВИЛА И ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ДЕЛОВЫХ ПАРТНЕРОВ ПРИ РАБОТЕ С ИНФОРМАЦИОННЫМИ РЕСУРСАМИ ОБЩЕСТВА 7**](#_Toc148704094)

[**4.1. ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ И ОБУЧЕНИЕ РАБОТНИКОВ 7**](#_Toc148704095)

[**4.2. ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ 7**](#_Toc148704096)

[**4.3. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 8**](#_Toc148704097)

[**5. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ В СЛУЧАЕ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (компьютерных атак) 9**](#_Toc148704098)

# 1. ВВОДНЫЕ ПОЛОЖЕНИЯ

## 1.1. ВВЕДЕНИЕ

1.1.1. Инструкция по информационной безопасности для Деловых партнеров ООО «КанБайкал» (далее – Общество, вместе – Инструкция) разработана и принята в соответствии с действующей в Обществе Политикой информационной безопасности.

1.1.2. Одним из основных видов деятельности Общества являются процессы, связанные с эксплуатацией автоматизированных систем управления технологическим процессом (АСУ ТП), информационно-телекоммуникационных и информационных систем.

1.1.3. Применение современных информационных технологий в бизнес-деятельности является неотъемлемым условием устойчивого и эффективного функционирования Общества. Информационные технологии имеют реальную ценность для Общества, в связи с чем информационные технологии нуждаются в адекватной защите от угроз, способных нарушить такие свойства информации, как конфиденциальность, целостность и доступность, что в свою очередь может снизить эффективность деятельности Общества и отрицательно повлиять на его деловую репутацию, привести не только к прямым финансовым потерям, но и к невыполнению требований законодательства РФ в области защиты информации.

1.1.4. Все положения настоящей инструкции, регламентирующие деятельность работников Деловых партнеров при работе с информационными активами Общества, обязательны к исполнению.

## 1.2. ЦЕЛИ

Настоящая инструкция разработана в целях:

- Реализации положений Политики информационной безопасности Общества в части взаимодействия Общества с его Деловыми партнерами и третьими лицами, имеющими с Обществом отношения;

- Предупреждения, либо максимально возможного уменьшения прямых и косвенных потерь Общества, связанных с реализацией угроз информационной безопасности со стороны Деловых партнеров и третьих лиц;

- защиты законных интересов владельцев информации, в том числе клиентов и партнеров Общества;

- повышения качества предоставляемых услуг и предоставления гарантий безопасности интересов клиентов.

## 1.3. ЗАДАЧИ

Основными задачами настоящей Инструкции являются:

* обеспечение безопасности бизнес-процессов Общества в условиях возрастающего уровня угроз, включая обеспечение оперативного мониторинга и оценку состояния защищенности как в периметре Общества, так и за его пределами;
* повышение эффективности защиты от спланированных целенаправленных компьютерных атак злоумышленниками;
* повышение информационной безопасности технологических и производственных систем;
* соответствие требованиям законодательства РФ в области информационной безопасности путем обеспечения заданного уровня информационной безопасности ИТ-активов;
* обеспечение непрерывности и комплексности, обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры.

## 1.4. ОБЛАСТЬ ДЕЙСТВИЯ

1.4.1. Действие настоящей Инструкции распространяется на всех работников сторонних организаций, связанных с ООО «КанБайкал» отношениями и имеющих доступ в информационные системы Общества.

1.4.2. Инструкция охватывает все информационные активы Общества, в том числе физические, сетевые, программные и информационные ресурсы, системы, сервисы, технологии и процессы, а также всех работников Общества, к которым в силу отношений Деловым партнерам и третьим лицам предоставлен доступ, и обеспечивает защиту от нарушения конфиденциальности, целостности и доступности, а также защиту ИТ-инфраструктуры от разрушения, повреждения, хищения или несанкционированной модификации ее элементов.

1.4.3. Нарушение действующего законодательства вследствие неисполнения настоящей Инструкции работниками сторонних организаций, влечет за собой ответственность в соответствии с законодательством Российской Федерации.

# 2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящая Инструкция представляет собой систематизированное изложение целей и задач защиты информации при двухстороннем взаимодействии Общества со сторонними организациями и третьими лицами, а также уточняет общую стратегию и базовые принципы обеспечения информационной безопасности в Обществе.

2.2. Инструкция по информационной безопасности является неотъемлемой частью корпоративной иерархической системы нормативного обеспечения Общества.

2.3. Положения настоящей Инструкции являются основой для принятия управленческих решений по надлежащей защите информационных активов и контролю за ее исполнением.

2.4. Информационная безопасность должна восприниматься клиентами, деловыми партнерами и работниками Общества как процесс, способствующий успешной деятельности по следующим направлениям:

* защита репутации Общества;
* повышение производительности бизнес-процессов;
* сокращение издержек, снижение операционных потерь;
* соответствие формальным требованиям;
* обеспечение непрерывности процесса обеспечения информационной безопасности.

# 3. ОБЪЕКТЫ ЗАЩИТЫ, ИНФОРМАЦИОННЫЕ АКТИВЫ

3.1. Объектом защиты для целей настоящей Инструкции является информационная сфера Общества, охватывающая его информационное взаимодействие с внешним миром.

3.2. Информационная сфера Общества, как объект защиты, представляет собой распределенную динамичную систему взаимодействующих материальных и нематериальных активов Общества, связанных с формированием, обработкой, распространением и использованием информации.

3.3. Информационные активы Общества подразделяются на следующие виды:

* *Люди* - руководство и работники Общества, работники организаций-партнеров, работники контролирующих государственных органов;
* *Процессы* - технологические процессы, информационные технологические процессы, процессы жизненного цикла автоматизированных систем, процессы управления и контроля;
* *Сервисы* - вычислительные и коммуникационные сервисы, другие технические сервисы (отопление, освещение, энергоснабжение, кондиционирование воздуха).
* *Информационные ресурсы* - базы данных и файлы данных, системная/техническая документация, руководства пользователя, учебные материалы, операционные процедуры и процедуры поддержки, планы обеспечения бесперебойной работы организации, процедуры перехода на аварийный режим;
* *Программные ресурсы* - прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты;
* *Физические ресурсы* - компьютеры и коммуникационное оборудование, магнитные носители данных (ленты и диски), другое техническое оборудование (блоки питания, кондиционеры), мебель, помещения.

# 4. ПРИНЦИПЫ, ПРАВИЛА И ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ДЕЛОВЫХ ПАРТНЕРОВ ПРИ РАБОТЕ С ИНФОРМАЦИОННЫМИ РЕСУРСАМИ ОБЩЕСТВА

## 4.1. ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ И ОБУЧЕНИЕ РАБОТНИКОВ

4.1.1. К работе с информационными ресурсами Общества должны допускаться только те работники сторонних организаций, которые на регулярной основе проходят обучение по информационной безопасности, обладают в достаточной степени приемами безопасной работы с вверенными им ИТ-активами и достаточным уровнем квалификации в области информационной безопасности.

4.1.2. Повышение осведомленности работников сторонних организаций, в области информационной безопасности должно быть направлено на эффективное усвоение работниками основных правил безопасной работы с информационными ресурсами.

4.1.3. Обучение должно проводиться как при приеме на работу или изменении в должностных обязанностях, так и на регулярной основе с документально установленной периодичностью.

4.1.4. Программа обучения в области информационной безопасности работников сторонних организаций, допускаемых к работе с информационными ресурсами Общества должна предусматривать не только теоретическую подготовку, но и проведение тестирования работников на знание основных правил и требований информационной безопасности.

## 4.2. ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ

4.2.1. Для любых защищаемых данных и документов в каждый конкретный момент времени должен быть однозначно определен круг лиц, которым санкционирован доступ к данным ресурсам в том минимальном объеме, который необходим этим лицам для исполнения своих должностных обязанностей.

4.2.2. Защищаемая информация должна использоваться работниками сторонних организаций только в и в рамках обязательств и полномочий, определенных для отведенной им роли. Запрещено использование информационных ресурсов, ИТ-сервисов и устройств, применение которых не связано с исполнением указанными работниками обязательств.

4.2.3. Требования по обеспечению безопасности конфиденциальной информации на бумажных носителях устанавливает служба безопасности Общества, для информации в электронном виде требования безопасности устанавливает отдел информационной безопасности. Передача конфиденциальной информации сторонним организациям, либо третьим лицам, с которыми Общество сотрудничает на временной или постоянной основе, допустима только в том случае, если с этими организациями, либо лицами заключены соответствующие взаимоотношения, а также соглашение о конфиденциальности.

4.2.4. Несанкционированный доступ к конфиденциальной информации, нарушение режима обработки конфиденциальной информации, включая ее несанкционированное раскрытие, передачу, искажение или уничтожение будет расцениваться как инцидент и, в зависимости от уровня тяжести последствий для Общества, может иметь правовые последствия для контрагента.

4.2.5. Общество устанавливает разрешительный порядок предоставления доступа к своим информационным ресурсам. Отдел информационной безопасности Общества, как ответственный за определение режима и поддержание необходимого уровня информационной безопасности, разрабатывает и внедряет соответствующие правила и процедуры, включая авторизацию и аудит доступа, устанавливает правила использования средств технической защиты информации, реализует необходимые контрольные меры.

## 4.3. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.3.1. Развитие информационной сферы Общества проходит в условиях воздействия различных факторов, стремящихся нарушить естественное и ожидаемое течение его информационных процессов. Различные факторы такого рода обобщенно определяются как угрозы информационной безопасности.

4.3.2. Угрозы информационной безопасности рассматриваются и выявляются на всех уровнях иерархической модели информационной инфраструктуры Общества, начиная с физического и заканчивая уровнем бизнес-процессов. При этом, относительно Общества всегда рассматриваются как внешние, так и внутренние угрозы.

# 5. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ В СЛУЧАЕ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (компьютерных атак)

5.1. С целью предупреждения и минимизации негативных последствий для информационно-технологических ресурсов Сторон должно незамедлительно осуществляться взаимное информирование об инцидентах информационной безопасности (в том числе компьютерных атаках), которые привели или могут привести к значительным негативным последствиям, в том числе для исполнения обязательств как для Общества, так и для его Деловых партнеров.

5.2. Взаимное информирование осуществляется между кураторами взаимоотношений по приоритетным каналам связи, указанным во взаимоотношениях.

5.3. По завершении ликвидации последствий инцидентов информационной безопасности необходимо выполнить внеплановую проверку состояния информационной системы, в который произошел инцидент.

5.4. Результаты проверки должны быть направлены другой Стороне в форме Акта.