START

УТВЕРЖЕНО

Приказом генерального директора

«21» февраля 2023 г.

Политика
Системы управления информационной безопасностью

(извлечение)

2023 г.

2.3 Термины, определения и сокращения

2.3.1 В Политике использованы следующие термины, определения и сокращения:

Термин/сокращение	Определение
Актив	Все, что имеет ценность для Компании. К Активам относятся: информационные системы, информация, программное обеспечение, оборудование, сервисы, работники Компании и т. д.
Владелец актива	Работник Компании, уполномоченный управлять созданием, разработкой, поддержанием, использованием и защитой Активов
Владелец процесса	Владелец соответствующего бизнес-процесса, предусмотренного моделью процессов Компании
Доступность	Свойство быть доступным и готовым к использованию по запросу авторизованного субъекта
Информация	Знания или данные, которые имеют значение для Компании
Информационная безопасность	Сохранение конфиденциальности, целостности и доступности информации
Комитет по ИБ	Коллегиальный орган, созданный в целях координации и контроля за организацией работ по обеспечению информационной безопасности в Компании, а также для принятия стратегических решений по развитию информационной безопасности в Компании.
Компания	
Конфиденциальность	Свойство информации быть недоступной или закрытой для неавторизированных лиц, сущностей или процессов
Область деятельности СУИБ	Область применения и границы СУИБ в контексте бизнес-процессов, подразделений Компании, территориальных площадок, ресурсов и применяемых технологий
Система управления информационной безопасностью	Часть общей системы управления Компании, предназначенная для разработки, внедрения, применения, мониторинга, анализа, поддержания и улучшения процессов обеспечения ИБ Компании. СУИБ включает организационную структуру, политику, планирование, обязанности участников процессов СУИБ, процессы и ресурсы в области ИБ
Целостность	Свойство сохранения правильности и полноты активов
ИБ	Информационная безопасность
ОД	Область деятельности
ПДн	Персональные данные
СУИБ	Система управления информационной безопасностью

3. Основные положения

3.1 Одним из важнейших Активов Компании является информация, значимая для ее деятельности, в том числе используемая в ходе взаимодействия с клиентами

и партнерами.

3.2 Нарушение применимых требований ИБ может привести к серьезным последствиям, таким как финансовые потери, правовые санкции, ущерб репутации Компании, в том числе потеря доверия со стороны клиентов и партнеров, снижение конкурентоспособности на международных рынках.

3.3 Надлежащий уровень ИБ в Компании обеспечивается в соответствии с требованиями бизнеса, требованиями законодательства и регуляторов в части ИБ путем внедрения и непрерывного совершенствования СУИБ на основе международных стандартов и практик.

4. Область деятельности СУИБ

4.1 Для эффективной реализации процессов обеспечения ИБ в Компании внедряется СУИБ, соответствующая требованиям международного стандарта ISO/IEC 27001:2013.

4.2 СУИБ должна, в первую очередь, распространяться на ключевые бизнес-процессы, безопасность и непрерывность которых важно обеспечить для стабильного функционирования всей Компании.

4.3 Описание бизнес-процессов, а также, входящих в него подразделений и активов, обоснование выбора бизнес-процессов в качестве области деятельности СУИБ, будут приведены в документе «Область применения системы управления информационной безопасностью».

5. Цели и задачи системы управления ИБ

5.1 Перечень активов Компании регулярно пересматривается и актуализируется в соответствии с процессом анализа рисков ИБ.

5.2 Основная цель СУИБ — создание и постоянное поддержание в Компании условий, при которых риски, связанные с обеспечением безопасности активов Компании, постоянно контролируются и находятся на приемлемом уровне.

5.3 Достижение данной цели позволяет:

- защитить Активы Компании от всех видов угроз (внешних и внутренних, умышленных и непреднамеренных);
- обеспечить непрерывность бизнеса;
- обеспечить соответствие Компании требованиям действующего законодательства и регуляторов в области ИБ;
- обеспечить соответствие процессов обеспечения ИБ бизнес-требованиям Компании;
- минимизировать ущерб, наносимый бизнесу в результате возникновения инцидентов ИБ;
- увеличить прибыли на инвестированный капитал и получить дополнительные возможности для бизнеса;
- обеспечить доверие клиентов и партнеров Компании.

5.4 Вышеописанная цель достигается решением следующих задач:

- инвентаризация активов Компании и регулярное проведение оценки рисков ИБ;
- применение обоснованных, экономически эффективных организационных и технических мер по обеспечению ИБ;
- выявление применимых требований действующего законодательства и регуляторов в области ИБ, достижение соответствия этим требованиям;
- установление ответственности работников по вопросам обеспечения ИБ, обучение и повышение их осведомленности в части ИБ;

- регулярная оценка соответствия СУИБ применимым внутренним и внешним требованиям посредством проведения внутренних аудитов СУИБ, мониторинга эффективности процессов СУИБ, анализа СУИБ руководством Компании;
- внедрение корректирующих действий в случае выявления отклонений или несоответствий в работе СУИБ внутренним и внешним требованиям;
- подтверждение соответствия СУИБ Компании требованиям международного стандарта ISO/IEC 27001:2013.

6. Принципы СУИБ

В процессе обеспечения ИБ Компания должна руководствоваться принципами, приведенными ниже:

6.1. **Законность.** При обеспечении ИБ выполняются требования применимого законодательства, а также действующие нормативные требования государственных регулирующих органов, в том числе, международных.

6.2. **Адекватность** существующим угрозам и экономическая обоснованность. Применяемые организационные и технические меры защиты выбираются исходя из потребностей бизнеса на основе результатов анализа и оценки рисков ИБ, в частности, анализа актуальных угроз и затрат на внедрение и сопровождение мер управления рисками. Проводится периодическая оценка эффективности используемых мер и механизмов защиты.

6.3. **Минимизация** ограничивающего влияния на бизнес-процессы. Применяемые организационные и технические меры СУИБ минимально влияют на функционирование и характеристики бизнес-процессов Компании.

6.4. **Перспективность** и ориентация на существующие российские и международные открытые стандарты. Организационные и технические меры СУИБ реализуются с учетом мировых тенденций в области ИБ. Ориентация на открытые стандарты позволяет использовать накопленный мировой опыт в области защиты информации, а также обеспечивает прозрачность процессов ИБ и простоту взаимодействия в рамках задач по обеспечению ИБ.

6.5. **Непрерывность функционирования**. Обеспечиваются отказоустойчивость, надежность, доступность и корректность функционирования организационных и технических мер СУИБ.

6.6. **Непрерывность совершенствования**. Для успешного противодействия угрозам ИБ в условиях постоянно меняющегося внешнего и внутреннего окружения реализуется непрерывный цикл развития и совершенствования СУИБ.

6.7. **Персональная ответственность**. Каждый работник Компании несет персональную ответственность за выполнение функций и требований, возложенных на него в рамках функционирования СУИБ.

6.8. **Контроль**. Осуществляется постоянный контроль выполнения работниками Компании требований в области ИБ.

7. Стратегическое управление СУИБ

7.1 Деятельность по обеспечению ИБ в Компании должна планироваться ежегодно на уровне высшего руководства. Ресурсы на поддержку и модернизацию СУИБ должны регулярно выделяться высшим руководством.

7.2 В целях координации действий структурных подразделений Компании по обеспечению ИБ должен быть сформирован коллегиальный орган, выполняющий функции контроля, анализа и совершенствования СУИБ — Комитет по ИБ.

7.3 Ответственность за ИБ должна быть четко определена и документирована.

8. Определение ролей и ответственности

8.1 Для достижения заявленных целей Компании в сфере ИБ для работников и представителей сторонних организаций должна быть определены роли и ответственность.

8.2 Требования к порядку назначения работников на роли, зонам их ответственности должны быть детально документированы в нормативных документах Компании.

9. Управление рисками

9.1 В соответствии с риск-ориентированным подходом, устанавливаемым Политикой, в Компании должны регулярно проводиться инвентаризация активов, категорирование информации, а также, анализ и оценка рисков в соответствии с разработанной процедурой управления рисками ИБ, которая предусматривает идентификацию, анализ и оценку рисков ИБ, обработку неприемлемых рисков.

9.2 Результаты оценки рисков, состав применяемых в Компании мер обеспечения ИБ и планы по обработке рисков должны быть сформированы в соответствии с принятой в Компании методикой по управлению рисками ИБ.

9.3 Ответственность за пересмотр рисков, разработку и контроль исполнения мероприятий по минимизации рисков, утверждение критериев принятия рисков ИБ должна быть определена и документирована.

10. Управление документацией СУИБ

10.1 Разработка, оформление, согласование, регистрация, хранение, передача и уничтожение документации, относящейся к СУИБ Компании, должны соответствовать принятым в Компании требованиям по управлению организационно-распорядительной документацией.

10.2 Доступ к документации, представленной как на печатных носителях, так и в электронном виде и содержащей конфиденциальную информацию, должен быть ограничен и предоставляться только тем работникам Компании, контрагентам и партнерам, которые прошли необходимые процедуры получения соответствующих прав доступа.

10.3 В поддержку организационно-распорядительной документации СУИБ Компании должны создаваться записи, которые являются свидетельствами выполнения процессов управления и обеспечения ИБ и результативности функционирования СУИБ Компании в целом.

11. Обучение персонала

11.1 Работники Компании должны регулярно проходить обучение (повышение уровня знаний) в области ИБ.

11.2 Работники Компании, ответственные за определение и контроль требований по ИБ, должны постоянно поддерживать уровень своей компетенции, принимая участие в различных выставках, форумах и конференциях по ИБ, изучая методики, признанные лучшими мировыми практиками, а также используя источники массовой информации.

11.3 Должен проводиться регулярный контроль знаний работников Компании в области ИБ.

12. Организация работы со сторонними организациями

12.1 Компания в процессе своей деятельности взаимодействует со следующими сторонними организациями:

- партнеры;
- заказчики (юридические лица);
- пользователи-физические лица;
- международные и российские регуляторы;
- государственные органы страны юрисдикции Компании;
- поставщики товаров и услуг.

12.2 При заключении договоров со сторонними организациями необходимо учитывать требования ИБ обеих сторон. Согласованные требования по ИБ, касающиеся порядка обмена, обработки, хранения и распространения информации, предоставления доступа сторонних организаций к активам Компании должны быть зафиксированы в договоре и/или соглашении о конфиденциальности.

12.3 В договоре с контрагентами, оказывающими услуги по обеспечению физической безопасности и обслуживанию ИТ-инфраструктуры Компании, должны быть учтены требования к порядку осуществления доступа на территорию, в помещения и к Активам Компании.

12.4 Взаимодействие с международными и российскими регуляторами, государственными органами регламентируются соответствующими федеральными законами и другими нормативно-правовыми актами Российской Федерации, применимым международным законодательством.

13. Внутренние аудиты ИБ

13.1 В Компании должны регулярно (не реже раза в год) проводиться внутренние аудиты СУИБ с целью проверки того, что процессы, процедуры и меры обеспечения ИБ:

- соответствуют требованиям нормативных документов СУИБ;
- соответствуют требованиям применимого международного и российского законодательства по ключевым бизнес-процессам;
- соответствуют требованиям ISO/IEC 27001:2013, а также требованиям действующего законодательства;
- реализованы и сопровождаются в соответствии с установленными целями и задачами ИБ.

13.2 Критерии, область аудита, частота, методы проведения, ответственность, требования к планированию и проведению аудитов в Компании, а также к предоставлению отчетов по результатам и ведению записей должны быть определены и документированы.

13.3 Выбор аудиторов и проведение аудитов должны гарантировать объективность и непредвзятость процесса аудита. Аудиторы не должны проверять свою собственную работу.

13.4 Выявленные в ходе внутренних аудитов несоответствия и их причины должны устраняться корректирующими мероприятиями.

13.5 Доступ к техническим средствам проведения аудита должен быть защищен с целью предотвращения возможного ненадлежащего использования и компрометации. Доступ к результатам аудита со стороны работников Компании и/или работников сторонних организаций должен быть ограничен.

14. Мониторинг, анализ эффективности и совершенствование процессов СУИБ

14.1 В Компании должен проводиться регулярный мониторинг процессов СУИБ с целью:

- быстрого обнаружения ошибок, отклонений и несоответствий в результатах обработки информации, выполнении процессов обеспечения и управления ИБ, а также выявления причин этих отклонений;
- быстрого выявления удавшихся и неудавшихся попыток нарушений и инцидентов ИБ;
- оценки эффективности мероприятий, предпринятых для совершенствования СУИБ (путем введения специальных показателей эффективности).

14.2 В Компании регулярно, не менее одного раза в год, должен проводиться анализ СУИБ. При этом должны учитываться результаты проведения аудитов безопасности, статистика и дополнительная информация по произошедшим инцидентам ИБ, результаты оценки эффективности процессов ИБ, а также предложения и комментарии от всех заинтересованных сторон.

14.3 В Компании должна непрерывно совершенствоваться СУИБ путем применения корректирующих мер, определенных по результатам анализа СУИБ. Порядок выбора, согласования и применения корректирующих мер должен быть документирован.

15. Соответствие требованиям законодательства

15.1 Защита права интеллектуальной собственности

15.1.1 В Компании должно обеспечиваться соблюдение требований законодательства и договорных отношений в области использования материалов, охраняемых правом интеллектуальной собственности, а также в области использования коммерческого программного обеспечения.

15.1.2 В Компании допустимо к использованию только законно введенное в оборот и легально реализуемое программное обеспечение.

15.2 Защита персональных данных

15.2.1 В Компании должны быть определены и реализованы требования к обработке и обеспечению безопасности персональных данных в соответствии с действующим применимым законодательством, требованиями и рекомендациями регулирующих органов.

15.2.2 Требования к сбору, систематизации, уточнению, хранению, использованию, распространению, обезличиванию, блокированию и уничтожению персональных данных должны быть определены в нормативных документах Компании.

16. Порядок внесения изменений

16.1 Ответственным за актуализацию Политики является специалист по информационной безопасности.

16.2 Политика пересматривается не реже, чем раз в три года.

16.3 Внеплановый пересмотр Политики может осуществляться также в следующих случаях:

- при существенном изменении организационной структуры Компании, структуры Активов и применения новых технологий передачи, хранения и обработки информации;
- по результатам проведения проверки соответствия ИБ (аудит, оценка эффективности);
- по результатам анализа произошедших инцидентов ИБ;
- по результатам анализа рисков ИБ.

17. Контроль за исполнением Политики

17.1 Контроль выполнения требований Политики

17.1.1 Все работники Компании несут дисциплинарную ответственность за несоблюдение требований Политики.

17.1.2 Контроль за соблюдением требований Политики в Компании осуществляет Генеральный директор.

18. Ответственность работников

18.1 В случае нарушения требований ИБ работник может быть привлечен к дисциплинарной, материальной, административной, уголовной ответственности в соответствии с законодательством Российской Федерации.