ООО «СОФТКЛУБ»

Редакция **23 сентября 2025**	**Деятельность**		
Разработал УИБ **Дата 23 сентября 2025**	Проверил **СМК** **Дата 23 сентября 2025**	№ файла **Политика ИБ**	Экземпляр **подлинник**

УТВЕРЖДАЮ

Генеральный директор

ООО «СОФТКЛУБ»

_____ В.Г. Сиротко

«23» сентября 2025г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Список изменений документа

Номер изменения	дата	ФИО инициатора	Изменения
1.0.0	15.01.2021	Ловчий А.Д.	Утверждена первая версия документа
1.0.1	19.04.2021	Ловчий А.Д.	Утверждена новая версия документа после внесенных изменений по результатам аудита БелГИМ
1.0.2	10.05.2024	Ловчий А.Д.	Утверждена новая версия документа после внесенных изменений в связи с Приказом ОАЦ от 25 июля 2023 № 130
1.0.3	17.01.2025	Ловчий А.Д.	Утверждена новая версия документа после внесенных изменений по результатам аудита БГЦА и в связи с Приказом ОАЦ 10 декабря 2024 г. № 259
1.0.4	02.04.2025	Ловчий А.Д.	Утверждена новая версия документа после принятия Рабочего регламента управления инцидентами ИБ
2.0.0	09.09.2025	Анищенко В.В.	Утверждена вторая версия документа
3.0.0	23.09.2025	Ловчий А.Д.	Утверждена третья версия документа

ОГЛАВЛЕНИЕ

1 НАЗНАЧЕНИЕ

Настоящий документ Политика информационной безопасности ООО «СОФТКЛУБ» (далее — Политика) является основополагающим документом, определяющим позицию, цели, задачи и принципы ООО «СОФТКЛУБ» (далее — Организация) в области информационной безопасности.

2 ОБЩИЕ ПОЛОЖЕНИЯ

Информационная безопасность — это совокупность сотрудников, политик, процессов и технологий, задействованных Организацией в целях защиты информационных активов. Защищенность информационных активов Организации характеризуется нейтрализацией актуальных угроз информационной безопасности техническими, организационными и правовыми мерами.

Под информационными активами для целей настоящей Политики признаются средства вычислительной техники, телекоммуникационное оборудование, системное и прикладное программное обеспечение, информационные ресурсы, входящие в состав информационной системы.

Деятельность Организации в области информационной безопасности основывается на стратегии развития ООО «СОФТКЛУБ», а решаемые задачи способствуют эффективному и безопасному развитию бизнеса ООО «СОФТКЛУБ».

Политика разработана в соответствии с законодательством Республики Беларусь в области защиты информации, положениями международных и национальных стандартов и передовых мировых практик.

3 ДЕКЛАРАЦИЯ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Принятием Политики Организация провозглашает и обязуется принимать надлежащие меры защиты информационных активов ООО «СОФТКЛУБ» от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности.

Руководство Организации осознает важность и необходимость совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства в области информационной безопасности, а также усложнения используемых информационных технологий.

Руководство Организации инициирует и контролирует работы в области информационной безопасности.

Руководство Организации принимает меры по обеспечению соответствия мер по защите информации требованиям, установленным законодательством Республики Беларусь.

Соблюдение принципов, правил и требований информационной безопасности является обязательным для всего персонала Организации.

Руководители и специалисты по информационной безопасности Организации должны ответственно выполнять свои обязанности, осознавая, что качество их работы непосредственно влияет на защищённость информационных активов Организации.

Каждый сотрудник Организации или партнера Организации несёт ответственность за выполнение требований информационной безопасности при работе с информационными активами Организации.

4 ЦЕЛИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обеспечение информационной безопасности Организации ориентировано на достижение следующих целей:

- Предоставление безопасной информационной среды для функционирования и развития бизнеса.
- Защита информационных активов от возможного нанесения ущерба посредством случайного или преднамеренного несанкционированного вмешательства в функционирование информационных систем Организации или несанкционированного доступа к обрабатываемым в них информационным активам и их неправомерного использования.
- Повышение конкурентоспособности, деловой репутации Организации путем снижения уровня риска в области информационной безопасности.
- Соответствие требованиям законодательства в области информационной безопасности и защиты персональных данных, а также соблюдение соответствующих договорных обязательств.

5 ЗАДАЧИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для достижения целей в области информационной безопасности Организацией решаются следующие задачи:

- прогнозирование, своевременное выявление угроз информационной безопасности и оперативное реагирование на них;
- защита от вмешательства в процесс функционирования информационных систем Организации лиц, не имеющих прав доступа к ним;
- разграничение доступа зарегистрированных пользователей к информационным активам;
- регистрация действий пользователей при использовании защищаемых информационных активов Организации в системных журналах и периодический контроль корректности действий пользователей путём анализа содержимого этих журналов;
- резервирование и архивирование информационных активов;
- защита от несанкционированной модификации и контроль целостности используемых программных средств;
- обеспечение непрерывности процессов деятельности и их восстановления после возможного прерывания;
- минимизация и локализация ущерба, наносимого интересам Организации реализацией угроз информационной безопасности и принятие соответствующих мер по их предотвращению;
- анализ функционирования систем обеспечения информационной безопасности, контроль защитных мер, оценка их эффективности;
- совершенствование системы защиты информации на основе анализа инцидентов информационной безопасности и оценки эффективности используемых защитных мер.

6 ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В Организации определены следующие принципы обеспечения информационной безопасности.

Принцип системности - Активы рассматриваются как взаимозависимые компоненты единой системы. Взаимовлияние компонентов учитывается при анализе рисков и угроз информационной безопасности.

Принцип законности - При выборе и реализации мер обеспечения информационной безопасности Организация строго соблюдает применимое законодательство, требования нормативных правовых и технических документов в области информационной безопасности.

Принцип полноты (комплексности) - В целях обеспечения информационной безопасности используется широкий спектр мер, методов и средств защиты, комплексное использование которых обеспечивает нейтрализацию актуальных угроз и отсутствие уязвимостей в точках интеграции.

Принцип эшелонированности - Недопустимо полагаться на один защитный рубеж. Система обеспечения информационной безопасности строится так, чтобы наиболее защищаемая зона безопасности находилась внутри других защищаемых зон.

Принцип равнопрочности - Эффективность защитных механизмов не должна быть сведена на нет слабым звеном, возникшим в результате недооценки угроз либо применения неадекватных мер защиты.

Принцип непрерывности - Обеспечение информационной безопасности является непрерывным целенаправленным процессом, предполагающим принятие мер защиты на всех этапах жизненного цикла активов.

Принцип персональной ответственности - Ответственность за обеспечение информационной безопасности возлагается на каждого сотрудника в пределах его полномочий.

7 ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПОЛИТИКИ

Сотрудники Организации обязаны выполнять требования и правила информационной безопасности при работе с информацией и информационными активами Организации, её партнёров и контрагентов, определённые в ЛПА Организации.

Распределение обязанностей сотрудников Организации и ответственность в области защиты информации определяется в ЛПА Организации.

Правила обеспечения информационной безопасности Организации обязательны для всех без исключения сотрудников Организации и должны учитываться во взаимоотношениях с партнерами и контрагентами.

Каждый сотрудник Организации за несоблюдение требований информационной безопасности несет дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с применимым законодательством.

Сотрудники партнёров и контрагентов, использующие информационные активы Организации, а также предоставленную им информацию, несут ответственность в соответствии с договорными отношениями, а также применимым законодательством.

8 ПЕРИОД ДЕЙСТВИЯ И ВНЕСЕНИЕ ИЗМЕНЕНИЙ

Настоящая Политика является локальным правовым актом постоянного действия. Настоящая Политика утверждается, изменяется и признается утратившей силу генеральным директором ООО «СОФТКЛУБ». Пересмотр Политики проводится на регулярной основе не реже одного раза в два года или по мере необходимости.

ЛИСТ СОГЛАСОВАНИЯ

Наименование документа и номер: Политика информационной безопасности – 3 редакция

Подразделение разработчик: Управление информационной безопасности

Ответственные участники Процесса должность, фамилия И.О.	Замечания	Подпись, дата
Заместитель генерального директора по науке и инновациям Анищенко В.В.		
Технический директор Коваленко В.В.		
Начальник управления информационной безопасности Ловчий А.Д.		