УТВЕРЖДЕНО/APPROVED

Совет директоров/ Board of Directors
October 22, 2021

Политика информационной безопасности/ Information Security Policy

1. Общие положения	1. General provisions
1.1. Назначение документа	**1.1. Document goal**
1.1.1. Настоящая политика информационной безопасности (далее – Политика) принадлежит ООО «Лента».	1.1.1. This Information Security Policy (hereinafter, the Policy) is owned by Lenta LLC.
1.1.2. Политика информационной безопасности является основополагающим документом, который определяет цели, принципы, подходы и методы обеспечения защищенности интересов ООО «ЛЕНТА» (далее – Компания) в информационной сфере, а также является декларацией намерения Руководства Компании поддерживать достижение целей и соблюдение принципов информационной безопасности (далее - ИБ) Компании.	1.1.2. The Information Security Policy is a framework document which defines purposes, principles, approaches and methods of protecting interests of Lenta LLC (hereinafter, the Company) in the information sphere, and is a declaration of the Company's Management intention to support achievement of the goals and compliance with the information security principles of the Company.
1.1.3. **Данный документ определяет:** 1.1.3.1. Комплексный подход к обеспечению информационной безопасности Компании в соответствии с требованиями бизнеса, норм законодательством РФ и при поддержке Руководства Компании; 1.1.3.2. Необходимые ресурсы, методы обеспечения и организации ИБ, нацеленные на защиту интересов Компании, основанные на требованиях законодательства РФ и лучших международных практиках (семейство стандартов ISO/IEC 27000); 1.1.3.3. Общие требования к информационной безопасности информационных активов Компании, а также порядок выполнения этих требований; 1.1.3.4. Укрепление необходимого уровня доверия к Компании в информационной сфере со стороны Государства, Акционеров, Клиентов, Партнеров и Сотрудников.	1.1.3. **This document defines:** 1.1.3.1. A complex approach to ensure the Company's information security in accordance with the business requirements, requirements of the Russian law and with the support of the Company's Management. 1.1.3.2. Necessary resources, methods to ensure and establish information security aiming to protect the Company's interests, based on the requirements of the laws of the Russian Federation and international best practices (family of standards ISO/IEC 27000); 1.1.3.3. General requirements for the information security of the Company's information assets, and the procedure for meeting these requirements. 1.1.3.4. Strengthening of the required level of confidence in the Company in the information sphere on the side of the government, stakeholders, customers, partners and employees.
1.1.4. Политика информационной безопасности должна быть доведена до сведения всех Сотрудников Компании в актуальной, доступной и понятной форме. 1.1.4.5. Допустимо также использование краткой выписки из Политики для публикации на общедоступных и корпоративных ресурсах.	1.1.4. The Information Security Policy must be communicated to all Employees of the Company in a relevant, user-friendly and understandable form. 1.1.4.1. A short excerpt from the Policy is also allowed for publication on public and corporate resources.
1.2. Область применения	**1.2. Scope**

1.2.1. Настоящая Политика распространяется на все виды информационных активов и на все бизнес-процессы Компании.	1.2.1. This Policy applies to all kinds of information assets and all business processes of the Company.
1.2.2. **Направления деятельности Компании в области информационной безопасности:**	1.2.2. **The Company's areas of activities in the sphere of information security:**
1.2.2.1 Создание, поддержка и развитие системы управления информационной безопасностью (СУИБ), соответствующей требованиям бизнеса, законодательства и лучшим мировым практикам.	1.2.2.1. Creation, support and development of the information security management system (ISMS) designed to comply with the requirements of the business, legislation and global best practices.
1.2.2.2 Прогнозирование, предупреждение, выявление, противодействие и нейтрализация внешних и внутренних угроз информационной безопасности, а также минимизация ущерба от их воздействия.	1.2.2.2. Forecasting, prevention, identification, counteracting and elimination of external and internal information security threats, as well as mitigation of damages arising from these threats.
1.2.2.3 Реализация комплекса мероприятий по обеспечению безопасности информационных систем, персонала, инфраструктуры, сетей передачи данных и носителей информации.	1.2.2.3. Implementation of the set of actions to ensure security of information systems, staff, infrastructure, networks of data transfer and information carriers.
1.2.2.4 Обеспечение выполнения и контроль соблюдения требований законодательства РФ и ЛНА в области информационной безопасности.	1.2.2.4. Enforcement and control over compliance with the legal requirements of the Russian Federation and internal regulations in the sphere of information security.
1.2.2.5 Повышение осведомленности персонала в области информационной безопасности.	1.2.2.5. Improvement of the employees' awareness in the sphere of information security.
1.2.3. Информация, представляющая ценность для Компании, ее бизнеса и Клиентов, защищается вне зависимости от способов ее обработки и формы представления.	1.2.3. The information valuable for the Company, its business and Customers is protected irrespective of the means of its processing and forms of its presentation.
1.2.4. Положения настоящей Политики дополняются и уточняются принятыми в Компании внутренними нормативными документами по информационной безопасности, такими как политики, процедуры, требования и инструкции.	1.2.4. The provisions of this Policy are supplemented and specified by the internal regulations adopted by the Company regarding information security, such as policies, procedures, requirements and instructions.
1.2.5. Сотрудники несут персональную ответственность за соблюдение настоящей Политики.	1.2.5. The employees are personally liable for compliance with this Policy.
1.2.5.1. В случае нарушения положений и требований настоящей Политики в соответствии с законодательством РФ к Сотрудникам могут применяться	1.2.5.1. If the Employees violate provisions and requirements of this Policy, they may be charged with criminal liability, administrative and disciplinary actions, including their

административные, уголовные и дисциплинарные меры, вплоть до увольнения.	dismissal, in accordance with the Russian laws.
1.2.5.2. Руководство Компании несет ответственность за внедрение настоящей Политики и мониторинг соблюдения её положений.	1.2.5.2. The Company's management is responsible for implementing this Policy and for monitoring compliance with its provisions.
1.2.6. Положения данного раздела детализированы в Требованиях по допустимому использованию информационных активов и ресурсов Сотрудниками.	1.2.6. The provisions of this section are specified in the Requirements on accepted use of information assets and resources by the Employees.
1.2.7. Основными классами информационных активов Компании, защиту которых необходимо обеспечить, являются:	1.2.7. The main classes of the Company’s information assets to be protected are as follows:
1.2.7.3. Информация на материальных носителях;	1.2.7.1. Information on physical media;
1.2.7.4. Информация, обрабатываемая в информационных системах Компании;	1.2.7.2. information processed in the Company’s information systems;
1.2.7.5. Программное обеспечение, входящее в информационные системы Компании;	1.2.7.3. Software included into the Company’s information systems;
1.2.7.6. Технические средства обработки информации, входящие в информационные системы Компании;	1.2.7.4. Technical means of processing of the information included into the Company’s information systems;
1.2.7.7. Средства и среды передачи информации;	1.2.7.5. Means and environment of information transmission;
1.2.7.8. Информационные и телекоммуникационные сервисы, предоставляемые Клиентам и Сотрудникам Компании;	1.2.7.6. Information and telecommunication services provided to the Company’s Customers and Employees;
1.2.7.9. Сотрудники Компании их квалификация, опыт и знания;	1.2.7.7. The Company’s employees, their skills, experience and knowledge;
1.2.7.10. Объекты интеллектуальной собственности, лицензии, репутация, имидж Компании;	1.2.7.8. Intellectual property objects, licenses, reputation, image of the Company;
1.2.7.11. Законодательные акты РФ определяют роль и требования к Компании как Обладателю информации и Оператору персональных данных.	1.2.7.9. The laws of the Russian Federation define the role and requirements to the Company as to the Information Holder and Personal Data Operator.
1.2.8. Компания**,** являясь Обладателем информации, обрабатываемой в КИС:	1.2.8. Being the Holder of the Information processed in the Corporate Information System, the Company:
1.2.8.1. Обязана обеспечивать и соблюдать конфиденциальность информации, доступ к которой ограничен федеральными законами;	1.2.8.1. Is required to ensure and protect confidentiality of the information which is limited-access information according to federal laws;
1.2.8.2. Обязана выполнять требования Контрагентов по защите информации,	1.2.8.2. Is required to meet the

являющейся их коммерческой тайной и переданной в Компанию; 1.2.8.3. Если иное не предусмотрено федеральными законами и требованиями договорных обязательств, имеет право самостоятельно разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа.	requirements of its Contractors on protection of the information which constitutes their trade secret and is transmitted to the Company; 1.2.8.3. Has the right to independently allow or restrict the access to the information, define the procedure and terms of such access, unless otherwise provided by the federal laws and respective contractual obligations.
1.2.9. Компания, являясь Оператором персональных данных: 1.2.9.1. Обязана выполнять требования государственных регуляторов и законодательства РФ в соответствии с федеральными законами и подзаконными актами в области обработки и защиты персональных данных; 1.2.9.2. Если иное не предусмотрено федеральными законами, самостоятельно определять порядок создания и эксплуатации информационных систем персональных данных.	1.2.9. Being the Personal Data Operator, the Company: 1.2.9.1. Is required to fulfill the requirements of the government regulators and laws of the Russian Federation in accordance with the federal laws and regulations in the sphere of personal data processing and protection; 1.2.9.2. Independently defines the procedure for creation and use of personal data information systems, unless otherwise provided by the federal laws.
2. Цели и принципы деятельности Компании в области информационной безопасности	**2. Goals and principles of the Company's activities in the sphere of information security**
2.1. Целью деятельности Компании в области информационной безопасности является обеспечение успешного выполнения Миссии и ключевых стратегических целей Компании, устойчивого функционирования бизнеса в условиях киберрисков.	**2.1.** The goal of the Company's activities in the sphere of information security is to ensure successful achievement of the Company's Mission and key strategic goals, sustainable business operation in cyber risk environment.
2.1.1. Киберриски способны привести: • К нарушению конфиденциальности, целостности, доступности обрабатываемой информации; • К нарушению устойчивости функционирования информационных систем и других информационных активов.	2.1.1. Cyber risks may lead to: • Compromise of confidentiality, integrity, accessibility of processed information; • Loss of stable operation of information systems and other information assets.
2.2. Цель, достигается путем предотвращения и минимизации потерь Компании: • от утечек конфиденциальной информации;	**2.2.** A goal to prevent and reduce the Company's losses from: • Leakage of confidential information;

• использования недостоверной, искаженной информации; • нарушения процессов обработки информации.	• Use of unreliable, distorted information; • Violation of information processing processes.
2.3. Для достижения указанных целей необходимо руководствоваться следующими принципами: **Бизнес-ориентированность** СУИБ должна соответствовать целям и ценностям бизнеса и защищать его интересы **Законность** Обеспечение ИБ должно осуществляться в соответствии с нормативно-правовыми актами в области ИБ и ЛНА Компании Процессы, связанные с обеспечением ИБ, должны выполняться на всех этапах жизненного цикла информации – от ее создания до уничтожения. Каждый Сотрудник на своем уровне должен принимать участие в процессах обеспечения ИБ. **Непрерывность** Принцип непрерывности определяет обеспечение ИБ как непрерывный процесс, направленный на снижение рисков уничтожения и повреждения значимых информационных активов Компании **Поддержка** Определяет необходимость обеспечения поддержки и лояльности Руководства и персонала Компании к мероприятиям ИБ. **Системность** Организационные меры и технические средства должны разрабатываться и применяться в рамках единой системы защиты, учитывающей все способы реализации актуальных угроз и не содержащей слабых мест на стыке отдельных ее компонентов.	**2.3.** To achieve these goals, the following principles should be used: **Focus on business** ISMS must correspond to the goals and values of the business and protect its interests **Legality** The information security must be ensured in compliance with legal and regulatory requirements in the sphere of information security and the Company's internal regulations The processes related to the information security must be embodied in all stages of the information life cycle – from its creation to its destruction. Each Employee at his/her level must take part in the processes of ensuring information security. **Continuity** The continuity principle defines information security as a continuous process aimed at reducing of the risks of destruction or damaging of important information assets of the Company. **Support** Defines the need in support and loyalty of the Management and staff of the Company to information security arrangements. **Consistency** Organizational and technical means must be developed and applied under the framework of the single protection system covering all sorts of materialization of current threats and free from cross-component weaknesses.

Своевременность Меры обеспечения защиты информации должны носить упреждающий характер.	**Timeliness** The measures of information protection must be preventive.
Комплексность Устанавливает согласованное применение различных методов и механизмов ИБ	**Overall perspective** Establishes approved application of different methods and mechanisms of information security
Разумная достаточность Обеспечивает сбалансированность между уровнем затрат на обеспечение ИБ с уровнем рисков информационных активов Компании	**Reasonable adequacy** Ensures the balance between the costs for information security and the risk level for information assets of the Company
Экономическая целесообразность Затраты на поддержку и развитие СУИБ не должны превышать размер ущерба от разглашения, утраты, уничтожения, искажения и несанкционированного доступа к информации	**Economic viability** The costs for support and development of ISMS must not exceed the damages from the information disclosure, loss, destruction, distortion and unauthorized access.
Ответственность Ответственность за обеспечение ИБ возлагается на каждого Сотрудника в пределах его функциональных обязанностей	**Responsibility** Each Employee within his/her scope of functions is responsible for ensuring of information security
Контроль Информационные ресурсы и средства коммуникаций должны предусматривать механизмы контроля порядка обращения с конфиденциальной информацией	**Control** Information resources and communication means must provide for controls applied to handling of confidential information
Простота использования и управляемость средств защиты Применение средств защиты не должно требовать специальных знаний или выполнения рутинных операций	**Usability and manageability of protection means** Using of protection means must not require special knowledge or exercise of routines
Централизация управления Процесс обеспечения ИБ осуществляется по организационной иерархии управления (по единым организационным, функциональным и методическим принципам).	**Centralized governance** The process of ensuring information security is carried out using organizational management hierarchy (using single organizational, functional and methodological principles).
	Back-up

Резервирование Все критичные процессы и сервисы должны предусматривать резервирование с учетом их постоянной готовности **Минимизация полномочий** Доступ к информационным ресурсам и технологиям должен быть ограничен, обоснован и предоставляться исключительно для выполнения служебных обязанностей **Постоянное совершенствование** СУИБ должна развиваться и совершенствоваться в соответствии с появлением новых векторов распространения угроз, изменениями в корпоративной информационной системе и нормативных актах, учитывать требования законодательства РФ и опираться на достигнутые результаты и лучшие мировые практики в области защиты информации.	All critical processes and services must be backed up in respect of their permanent readiness **Authority minimizing** The access to information resources and technologies must be minimized, motivated and provided only for business purposes **Ongoing improvement** ISMS must be developed and improved in compliance with newly appearing threats, changes in the corporate information system and regulations, requirements of the Russian laws and must be based on achieved results and best practices in the sphere of information protection.
3. Система Управления информационной безопасностью Компании	**3. Information management system of the Company**
3.1. Состояние защищенности интересов Компании в информационной сфере достигается созданием СУИБ, которая обеспечивает решение следующих задач: 3.1.1. Создание организационной структуры системы управления ИБ Компании; 3.1.2. Реализация процессов управления и обеспечения ИБ; 3.1.3. Реализацию методов, а также эффективное использование механизмов и средств обеспечения ИБ Компании. 3.1.4. Своевременное определение актуальных угроз ИБ и постоянное совершенствование процессов управления и обеспечения ИБ. **3.2.** Результативное управление процессами обеспечения информационной безопасности достигается использованием	**3.1.** The Company's interests in the information sphere are protected by the ISMS which is designed to address the following objectives: 3.1.1. Creation of the organizational structure for the ISMS of the Company; 3.1.2. Implementation of information security management and maintenance system; 3.1.3. Implementation of methods and effective use of mechanisms and means of maintenance of the Company's information security. 3.1.4. Timely detection of relevant threats to information security and on-going improvement of information security management and maintenance processes. **3.2.** The efficient managing of information security processes is achieved using process approach in compliance with

процессного подхода в соответствии со стандартом ISO\IEC 27001.	the standard ISO\IEC 27001.
3.3. Для реализации процессного подхода в Компании функционирует СУИБ, обеспечивающая приемлемый для защиты интересов Компании уровень ИБ, а также гарантирующая необходимый уровень доверия со стороны государства, акционеров, клиентов, партнеров и Сотрудников.	**3.3.** To implement the process approach, the Company operates ISMS ensuring acceptable level of information security to protect the Company's interests, and providing a required level of confidence from the government, stakeholders, customers, partners and Employees.
3.4. В интересах функционирования СУИБ в Компании реализуются следующие процессы:	**3.4.** The following processes are carried out to operate the ISMS in the Company's interests:
3.4.1. **Создание СУИБ:**	3.4.1. **ISMS development:**
3.4.1.1. Создание СУИБ и постоянное ее совершенствование согласно актуальным угрозам кибербезопасности и стратегии развития бизнеса;	3.4.1.1. Development of ISMS and its ongoing improvement according to the current cyber threats and business development strategy;
3.4.1.2. Разработка Политики ИБ, нормативных документов СУИБ и их пересмотр;	3.4.1.2. Development of Information Security Policy, ISMS-related regulations and their review;
3.4.1.3. Управление рисками - проведение оценки и обработки рисков кибербезопасности.	3.4.1.3. Risk management – assessment and handling of cyber security risks.
3.4.2. **Внедрение и эксплуатация СУИБ:**	3.4.2. **Implementation and operation of ISMS:**
3.4.2.1. Формирование плана обработки рисков СУИБ - разработка плана обработки рисков СУИБ и его актуализация;	3.4.2.1. Development of the schedule for ISMS risks handling – creating of the schedule for ISMS risks handling and its update;
3.4.2.2. Инициация выполнения задач - своевременное выполнение задач, определенных в планах обработки рисков, корректирующих и предупреждающих действий;	3.4.2.2. Initiation of task performing – timely performing of tasks defined in the schedules of risk handling, corrective and preventive actions;
3.4.2.3. Контроль выполнения задач - контроль выполнения активных задач;	3.4.2.3. Control over tasks performance – control over performing of active tasks;
3.4.2.4. Определение метрик эффективности СУИБ - разработка метрик эффективности мер, применяемых в СУИБ, и их актуализация;	3.4.2.4. Defining ISMS efficiency metrics – defining metrics to assess efficiency of measures used in ISMS, and their update;
3.4.2.5. Планирование ресурсов необходимых для эффективного функционирования СУИБ;	3.4.2.5. Planning of resources required for efficient operation of ISMS;
3.4.2.6. Выделение ресурсов, необходимых для устойчивого функционирования СУИБ;	3.4.2.6. Allocation of resources required for sustainable operation of ISMS;
3.4.2.7. Управление документацией - документирование порядка разработки, функционирования и совершенствования СУИБ и определение порядка обращения с документацией;	3.4.2.7. Documentation management – documentation of the procedure for development, operation and improvement of ISMS and defining the procedure for documentation handling;
3.4.2.8. Управление записями- определение состава и порядка документирования необходимых записей СУИБ;	3.4.2.8. Records management – defining composition and procedure for documenting of required records in ISMS;
3.4.2.9. Эксплуатационные процессы (включая	3.4.2.9. Maintenance processes (including

управление инцидентами ИБ]) - документирование и реализация всех эксплуатационных процессов СУИБ, созданных в результате внедрения выбранных мер обеспечения ИБ. 3.4.3. **Мониторинг и анализ СУИБ:** 3.4.3.1. Анализ СУИБ - общий анализ адекватности мер, реализованных в СУИБ; 3.4.3.2. Аудит СУИБ - проведения независимых аудитов СУИБ. 3.4.4. **Сопровождение и совершенствование СУИБ:** 3.4.4.1. Корректирующие действия- разработка корректирующих действий, направленных на устранение причин выявленных несоответствий для предотвращения их повторного возникновения или корректирующих действий, связанных с предложениями по совершенствованию СУИБ; 3.4.4.2. Предупреждающие действия - разработка предупреждающих действий, направленных на устранение причин потенциальных несоответствий или других потенциально нежелательных ситуаций, связанных с функционированием СУИБ.	IS incidents management]) – documenting and implementation of all maintenance processes of ISMS created as a result of implementation of selected measures of information security. 3.4.3. **ISMS monitoring and analysis:** 3.4.3.1. ISMS analysis – general analysis of adequacy of measures implemented in ISMS; 3.4.3.2. ISMS audit – independent audits of ISMS. 3.4.4. **ISMS support and improvement:** 3.4.4.1. Corrective actions – development of corrective actions aimed at elimination of the reasons for detected deficiencies to prevent their occurrence or corrective actions related to suggestions of ISMS improvement; 3.4.4.2. Preventive actions – development of preventive actions aimed at elimination of the reasons for potential deficiencies or other potentially unwanted situation related to the operation of ISMS.
4. Основные методы обеспечения информационной безопасности	**4. Key methods of ensuring information security**
4.1. Основные методы обеспечения ИБ объединяются по следующим направлениям: 4.1.1. Нормативно-правовые; 4.1.2. Организационные; 4.1.3. Технические; 4.1.4. Финансово-экономические. **4.2.** Основными нормативно-правовыми методами являются: 4.2.1. Создание и совершенствование ЛНА Компании, регулирующих отношения в области обеспечения ИБ. 4.2.2. Оценка результативности применения действующих ЛНА и выработку программы их совершенствования; 4.2.3. Создание организационно-правовых	**4.1.** The key methods to ensure information security are divided into the following areas: 4.1.1. Regulatory and legal; 4.1.2. Organizational; 4.1.3. Technical; 4.1.4. Financial and economic. **4.2.** The key regulatory and legal methods are: 4.2.1. Creation and improvement of the Company's internal regulations in the sphere of information security. 4.2.2. Assessment of the efficiency of using current internal regulations and development of the program of their improvement; 4.2.3. Creation of organizational and legal

механизмов обеспечения ИБ; 4.2.4. Определение ролей всех субъектов отношений в информационной сфере, включая пользователей информационных систем и сетей связи, установление их ответственности за соблюдение требований; 4.2.5. Разработка процессов, определяющих организацию расследования инцидентов ИБ; 4.2.6. Разработка подходов и методов категорирования информации, относимой к коммерческой тайне и персональным данным Компании; **4.3.** Основными организационными методами являются: 4.3.1. Создание и совершенствование СУИБ Компании; 4.3.2. Участие в научных исследованиях в области обеспечения ИБ в интересах отрасли и Компании; 4.3.3. Разграничение и делегирование полномочий в области обеспечения ИБ между подразделениями Компании; 4.3.4. Использование системы страхования информационных рисков для значимых активов Компании; 4.3.5. Координация деятельности подразделений Компании, решающих задачи обеспечения ИБ; 4.3.6. Контроль деятельности подразделений Компании, решающих задачи обеспечения ИБ и Сотрудников Компании в области обеспечения ИБ; 4.3.7. Предупреждение, выявление и пресечение инцидентов ИБ, связанных с посягательствами на законные интересы, активы и ресурсы Компании; 4.3.8. Совершенствование системы подготовки кадров, участвующих в обеспечении ИБ Компании. **4.4.** Основными методами в техническом направлении являются: 4.4.1. Проведение единой Политики в области обеспечения ИБ Компании; 4.4.2. Внедрение систем предотвращения несанкционированного доступа к обрабатываемой информации и специальных	mechanisms to ensure information security; 4.2.4. Defining roles of all related parties in the information environment, including users of information systems and communication networks, defining their responsibility for compliance with the requirements; 4.2.5. Development of processes to define arrangement of investigations into information security incidents; 4.2.6. Development of approaches and methods to categorize information treated as trade secret and personal data of the Company; **4.3.** The main organizational methods are as follows: 4.3.1. Creation and improvement of the Company's ISMS; 4.3.2. Participation in research in the sphere of ensuring information security in the interests of the industry and the Company; 4.3.3. Distribution and delegation of authorities in the sphere of information security among the Company's departments; 4.3.4. Using of the information risk insurance system for important assets of the Company; 4.3.5. Coordination of activities of the Company's departments engaged in information security assurance; 4.3.6. Control of the Company's departments engaged in information security assurance and the Company's Employees in information security; 4.3.7. Prevention, identification and suppression of information security incidents related to infringement on the Company's legal interests, assets and resources; 4.3.8. Improvement of the system of training for personnel engaged in information security assurance. **4.4.** The main technical methods are as follows: 4.4.1. Adopting of a single Policy in the sphere of information security; 4.4.2. Implementation of systems to prevent unauthorized access to processed information and special effects causing destruction, disposal, distortion of information, as well as changes in the normal

воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования информационных систем и систем связи; 4.4.3. Анализ возможности использования, внедрение и организация эксплуатации средств защиты информации и контроля результативности этих средств; 4.4.4. Создание системы сбора и анализа данных об источниках угроз ИБ активам Компании, а также о последствиях их осуществления; 4.4.5. Формирование системы мониторинга показателей и характеристик состояния ИБ Компании. **4.5.** Основными финансово-экономическими методами являются: 4.5.1. Разработка программ обеспечения ИБ Компании и определение порядка их финансирования; 4.5.2. Совершенствование системы финансирования работ, связанных с реализацией нормативно – правовых, организационных и технических методов защиты информации.	operation of information and communication systems; 4.4.3. Analysis of the possibility to use, implement and maintain the means of information protection and control over the efficiency of such means; 4.4.4. Creation of the system for collection and analysis of the data on the sources of information security threats to the Company's assets, and the consequences of their materialization; 4.4.5. Developing of the system to monitor the Company's information security indicators and properties. **4.5.** The main financial and economic means are as follows: 4.5.1. Development of the programs to ensure information security of the Company and definition of the procedure for their financing; 4.5.2. Improvement of the system of financing for the works related to implementation of regulatory, legal, organizational and technical methods of information protection.
5. Организационная структура Системы управления информационной безопасностью	**5. Organizational structure of the Information Security Management System**
5.1. Организационная структура системы управления ИБ Компании строится на основе разграничения функциональных полномочий между подразделениями и закрепляется в соответствующих нормативных документах, в части касающихся ИБ. **5.2.** Основными элементами организационной структуры системы управления ИБ являются: 5.2.1. Генеральный директор Компании; 5.2.2. Комиссия по защите информации; 5.2.3. Дирекция по обеспечению бизнеса; 5.2.4. Управление информационной безопасностью ДОБ (далее УИБ ДОБ) 5.2.5. Дирекция по информационным	**5.1.** Organizational structure of the information security management system of the Company is based on distribution of functional authorities among departments and is documented in the respective regulations related to the information security. **5.2.** The key elements of the organizational structure of the information security management system are: 5.2.1. CEO of the Company 5.2.2. Information protection committee 5.2.3. Business Support 5.2.4. Information Security Management, Security 5.2.5. IT;

технологиям; 5.2.6. Организации, которые на основании договоров, выполняют работы или оказывают услуги в области обеспечения ИБ Компании (далее - Подрядчики); 5.2.7. Иные Сотрудники подразделений Компании, принимающие в соответствии с локальными нормативными актами участие в решении задач обеспечения ИБ Компании (далее - Сотрудники). **5.3.** Генеральный директор Компании как обладатель информации: • Утверждает состав и объем информации, составляющих коммерческую тайну; • Утверждает перечень персональных данных, обрабатываемых в компании; • Определяет направление развития ИБ компании по предложениям УИБ; • Утверждает процедуру управления рисками ИБ. **5.4.** Комиссия по защите информации является постоянно действующим органом, принимающим управленческие решения в отношении защищаемой информации Компании и обеспечивающим постоянное совершенствование организационно-технических мер ее защиты. **5.5.** Дирекции по обеспечению бизнеса: • Разрабатывает и реализует стратегию информационной безопасности; • Разрабатывает ЛНА в области обеспечения ИБ; • Разрабатывает предложения по совершенствованию СУИБ; • Координирует деятельность всех подразделений Компании в области обеспечения ИБ с учетом определенных Генеральным директором приоритетных направлений развития бизнеса и действующего законодательства в области ИБ; • Формирует предложения в проект бюджета Компании на обеспечение ИБ; • Проводит работу по выявлению и оценке угроз и рисков ИБ, реализует меры по	5.2.6. Contracted companies engaged for performing of works or rendering of services in the sphere of the Company's information security (hereinafter, Contractors); 5.2.7. Other Employees of the Company taking part in addressing of the Company's information security issues in accordance with internal regulations (hereinafter, the Employees). **5.3.** Being the information holder, the CEO of the Company: • Approves the composition and the volume of information constituting trade secret; • Approves the list of personal data processed in the company; • Defines the direction for the company's information security development according to suggestions from the information security management; • Approves the procedure for information security risk management. **5.4.** The Information protection committee is a permanently operating body which takes management decisions in relation to the Company's protected information and ensures on-going improvement of organizational and technical measures of information security protection. **5.5.** Business Support: • Develop and implement the strategy of information security; • Develop internal regulations in the sphere of information security; • develop suggestions on improvement of ISMS; • Coordinate activities of all the Company's departments in the sphere of information security considering priority business directions defined by the CEO and the applicable laws in the sphere of information security; • Compile suggestions into the Company's draft budget for information security; • Detect and assess information security threats and risks, implement the measures to prevent information security

предотвращению угроз ИБ; • Контролирует реализацию требований по ИБ; • Организует мониторинг состояния ИБ, а также мониторинг атак на информационные активы Компании; • Инициирует и проводит расследования по фактам инцидентов ИБ; • Отвечает за внедрение, контроль, эксплуатацию программно-технических средств защиты информации, используемых в Компании; • На периодической основе информирует Генерального директора и Совет Директоров Компании о состоянии защищенности информационных активов, общем уровне защищенности, значимых инцидентах ИБ; • Представляет интересы Компании и взаимодействует с государственными, правоохранительными органами и регуляторами по вопросам ИБ в рамках своих полномочий и зоны ответственности; • Оказывает информационную поддержку Сотрудникам по вопросам информационной безопасности; • Содействует в организации обучения Сотрудников компании в области информационной безопасности, участвует в разработке обучающих курсов по информационной безопасности. 5.5.1. УИБ ДОБ является подразделением, ответственным за контроль обеспечения ИБ Компании. • Осуществляет совместно с ДИТ мониторинг состояния ИБ, а также мониторинг атак на информационные активы Компании. • Руководит работами по обеспечению ИБ Компании, • Санкционирует действия по обеспечению ИБ, • Определяет приоритетные направления развития ИБ Компании,	threats; • Control implementation of information security requirements; • Organize information security monitoring, and monitoring of attacks on the Company's information assets; • Initiate and conduct investigations on information security incidents; • Is responsible for the implementation, control, maintenance of software and hardware tools of information security used in the Company; • On a permanent basis, inform the CEO and the Board of Directors of the Company on the security of information assets, general security, significant information security incidents; • Represent the Company's interest and interact with the government, law-enforcement authorities and regulators in information security sphere within the scope of their responsibility and authority; • Provide information support to the EmployeeS ON INFORMATION SECURITY ISSUES; • Help in organization of the Company's employees training in the sphere of information security, take part in development of training courses on information security. 5.5.1. Information Security in Security is a department responsible for the control over the Company's information security. • Jointly with IT performs monitoring of information security and monitoring of threats on the Company's information assets; • Management of the works to ensure the Company's information security; • Authorize activities for information security maintenance; • Define priority development directions for the Company's information security;

• Формирует матрицу рисков ИБ, • Отвечает за подготовку и предоставление Директору по обеспечению бизнеса и Генеральному директору Компании отчетности по вопросам информационной безопасности. **5.6.** Дирекция по информационным технологиям: • Реализует технические мероприятия по информационной безопасности; • Разрабатывает предложения по совершенствованию СУИБ и выносит их на обсуждение и рассмотрение в УИБ; • Участвует в формировании бюджета на обеспечение ИБ Компании; • Согласно зоне ответственности, проводит работу по выявлению и оценке угроз и рисков ИБ, реализует меры по предотвращению угроз ИБ по представлениям УИБ; • Контролирует реализацию требований по ИБ в своей зоне ответственности; • Осуществляет совместно с УИБ мониторинг состояния ИБ, а также мониторинг атак на информационные активы Компании; • Участвует в проведении расследований по фактам инцидентов ИБ; • Отвечает за внедрение и контроль эксплуатации базовых программно-технических средств защиты информации, используемых в Компании; • Информирует УИБ о всех выявленных недостатках в системах защиты и инцидентах ИБ; • Представляют доступ к информационным активам Компании в соответствии с ЛНА по управлению доступом; • Обеспечивает соблюдения требований информационной безопасности для информационных систем при их внедрении и эксплуатации; • Реализует мероприятия по устранению	• Prepare the matrix of information security risks; • Responsibility for preparing and presentation of the information security reporting to the Business Support Director and CEO of the Company. **5.6.** IT: • Implement technical arrangements in information security; • Develop suggestions on improvement of ISMS and submit them for discussion and review by the Information Security Management; • Participates in drafting of the budget for information security of the Company; • According to the responsibility scope, detect and assess information security threats and risks, implement measures to prevent information security threats as defined by the Information Security Management; • Control over implementation of information security requirements within its responsibility scope; • Jointly with Information Security Management performs monitoring of the information security and monitoring of attacks to the Company's information assets; • Take part in investigations of the information security incidents; • Responsibility for implementation and control over the operation of basic software and hardware tools of information protection used in the Company; • Inform the Information Security Management on the defects detected in protection systems and information security incidents; • Provide access to the Company's information assets in accordance with internal regulations on the access management; • Ensure compliance with the information security requirements for information systems upon their implementation and operation; • Implement arrangements to address weaknesses of the Company's

уязвимостей информационных активов Компании, информирует УИБ о выявленных уязвимостях. **5.7.** Для реализации мероприятий в области ИБ Компания может привлекать на договорной основе Подрядчиков. **5.8.** Сотрудники в рамках своих полномочий выполняют требования по обеспечению ИБ, определенных в соответствующих ЛНА Компании. **5.9.** В Компании организованы процессы формирования и предоставления отчетности по вопросам ИБ: • По анализу защищенности и результатам тестирования на проникновение в информационные системы и активы Компании; • О сканировании инфраструктуры Компании на уязвимости и отчеты об их устранении; • По результатам аудитов ИБ и соблюдения требований законодательства РФ; • О выполнении планов мероприятий по ИБ; • По инцидентам ИБ; • По совершенствованию СУИБ. **5.10.** Порядок подготовки отчетов по вопросам ИБ, сроки их предоставления и ответственные за их подготовку определены в ЛНА Компании, в части касающихся ИБ, а также в должностных инструкциях участников СУИБ. **5.11.** В целях обеспечения информационной безопасности в Компании выделены ключевые обязанности и их исполнители в рамках процессов ИБ, которые приведены в матрице ответственности.	information assets, inform the Information Security Management on identified weaknesses. **5.7.** To implement arrangement in the sphere of information security, the Company may engage Contractors on a contract basis. **5.8.** The Employees meet the requirements to information security as defined in the respective internal regulations of the Company within the scope of their responsibility. **5.9.** The Company has the processes for preparing and presentation of the reporting on information security issues: • On analysis of protection and results of tests for penetration into the Company's information systems and assets; • On scanning of the Company's infrastructure for weaknesses and reports on elimination of weaknesses; • On the results of information security audits and compliance with the requirements of the Russian laws; • On execution of the schedules of information security arrangements; • On information security incidents; • On ISMS improvement. **5.10.** The procedure for information security reporting, timeframes for reports submitting and persons responsible for their preparation are defined by the Company's internal regulations, and job descriptions of ISMS participants. **5.11.** To ensure information security, the Company provides for the key responsibilities and their action holders within the information security processes which are specified in the responsibility matrix.
6. Документы, дополняющие Политику информационной безопасности	**6. Documents supplementing the Information Security Policy**
6.1. В Компании введен пропускной режим, порядок предоставления доступа. **6.2.** Компания может предоставлять Сотрудникам и Контрагентам удаленный доступ к своей корпоративной сети и информационным	**6.1.** The Company has the access control, the procedure of access provision. **6.2.** The Company may provide remote access to its corporate network and information systems to Employees and

системам.	Contractors.
6.3. Сотрудники и Контрагенты несут ответственность за сохранность и целостность предоставленных им Компанией активов.	**6.3.** Employees and Contractors are responsible for the safety and integrity of the assets provided by the Company.
6.4. В Компании допускается использование только разрешенного ПО.	**6.4.** The Company allows using only permitted software.
6.5. Компания обеспечивает защиту своих информационных активов, информационных систем и ИТ-оборудования от вирусов и иного вредоносного кода.	**6.5.** The Company protects its information assets, information systems and IT equipment from viruses and other malware code.
6.6. В Компании используется централизованная система резервного копирования информационных систем, серверов и баз данных.	**6.6.** The Company uses centralized backup system for information systems, servers and databases.
6.7. При использовании социальных сетей, облачных хранилищ и мессенджеров в Компании и за ее пределами Сотрудникам необходимо придерживаться принципов поведения.	**6.7.** The Employees using social networks, cloud storages and messengers in the Company and outside it must adhere to the rules.
6.8. Сотрудникам Компании запрещено делать заявления для средств массовой информации, а также для прочих внешних аудиторий в рамках деловых и прочих публичных мероприятий (конференции, форумы, круглые столы, совещания в органах власти с участием СМИ и пр.) от имени Компании, за исключением случаев, когда это регламентировано / согласовано Директором по связям с общественностью и государственными органами.	**6.8.** The Company's Employees are prohibited to make announcements on the Company's behalf for media and other external recipients as a part of business and other public events (conferences, forums, round tables, meetings in government authorities with media coverage, etc.), except for the cases provided /approved by the Public and Government Relations Director.
6.9. В Компании определена методология оценки рисков информационной безопасности.	**6.9.** The Company has a methodology for information security risk assessment.
6.9.1. Оценка рисков информационной безопасности базируется на общем подходе к оценке рисков в основной хозяйственной деятельности.	6.9.1. The information security risk assessment is based on the common approach to business risks assessment.
6.10. В Компании регламентирован порядок управления инцидентами информационной безопасности.	**6.10.** The Company has regulations for the procedure of information security incident management.
6.11. В Компании должны на регулярной основе проводиться сканирования на уязвимости и тестирование на проникновение в информационные системы и корпоративную сеть, устранение обнаруженных уязвимостей должно производиться в соответствии с уровнем их критичности.	**6.11.** The Company must be regularly scanned for weaknesses and tested for penetration to the information systems and corporate network, detected defects must be eliminated in accordance with the level of their severity.
6.12. В Компании должны регулярно проводиться аудиты информационной безопасности.	**6.12.** Regularly audits of the information security of the Company are required.
	6.13. Requirements to the information

6.13. Требования по ИБ, касающиеся порядка обмена, обработки, хранения и распространения конфиденциальной информации и порядка предоставления доступа контрагентам к информационным системам и активам Компании, должны быть определены в условиях проведения тендера с привлечением экспертизы УИБ ДОБ. **6.14.** ЛНА, разрабатываемая в структурных подразделениях Компании и раскрывающая более детально процессы обеспечения ИБ, не должна противоречить требованиям данной Политики.	security related to the procedure of exchange, processing, keeping and distribution of confidential information and the procedure of providing access to information systems and assets of the Company to contractors must be defined in tender terms with the expertise of the Information Security Management. **6.14.** An internal regulation developed in the Company's departments and specifying the processes of information security must not contradict to this Policy.
7. Термины и сокращения	**7. Terms and abbreviations**
Жизненный цикл информации Время движения ее от момента создания до момента получения пользователем и уничтожения или хранения на каких-либо носителях информации, но не использование или крайне редкое ее использование.	**Information life cycle** Evolution of the information from its creation to the receipt by the user and deletion or storage on any information media, but no using or very rare using of it.
Защищаемая информация Это информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями нормативных документов или требованиями, устанавливаемыми собственниками информации. К защищаемой информации относятся сведения о коммерческой тайне, обрабатываемых в Компании персональных данных, указанные соответствующих утвержденных Перечнях - Информации, составляющей коммерческую тайну ООО «Лента», а также Перечне персональных данных, обрабатываемых в ООО «Лента».	**Protected information** Information which is owned and is to be protected in accordance with the requirements of applicable regulations or requirements established by the information owners. Protected information includes trade secret, personal data processed in the Company, those specified in the approved lists of trade secrets of Lenta LLC, and the list of personal data processed in Lenta LLC.
Информационный Актив Все что имеет ценность для Компании в информационной сфере (информация, программное обеспечение, технические средства обработки информации, средства связи, сотрудники и прочее).	**Information asset** Everything which is meaningful for the Company in information sphere (information, software, technical means of information processing, communications means, employees, etc.)
Информационная безопасность (ИБ) Состояние, при котором обеспечивается безопасность информации и	**Information security** The state ensuring security of information and automated means of information processing.

автоматизированных средств ее обработки.	
Информационная система Система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию (ISO/IEC 2382:2015).	**Information system** System designed for storage, search and processing of information, and the relevant organizational resources (HR, technical, financial, etc.) providing and distributing information (ISO/IEC 2382:2015).
Информационные технологии (ИТ) Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.	**Information technologies** Processes, methods of search, collection, storage, processing, provision, distribution of information, and the means for such processes and methods.
Информация Сведения (сообщения, данные) независимо от формы их представления.	**Information** Data (messages, evidences) irrespective of the form of their presentation.
Корпоративная информационная система (КИС) Это комплексная автоматизированная система управления финансово-хозяйственной деятельностью предприятия, обеспечивающая принятие обоснованных управленческих решений на основе качественной и достоверной информации, получаемой с помощью современных управленческих и информационных технологий.	**Corporate information system** Complex automated system for the business activity management of an enterprise which enables to take reasonable management decisions based on quality and reliable information delivered using modern management and information technologies.
Конфиденциальная информация Это сведения, предоставленные в электронном или бумажном виде, которые запрещено передавать третьим лицам без ведома правообладателя.	**Confidential information** The data provided in electronic or paper form which are prohibited for transmission to third parties without their owner’s consent.
Коммерческая тайна Режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.	**Trade secret** A regime of the information confidentiality which allows its owner to increase incomes, avoid unreasonable expenses, keep its position on the market of goods, works, services or receive any other commercial benefit with the existing or possible circumstances.
Локально-нормативный акт (ЛНА) Это документы, которые устанавливают нормы труда в компании. В этих актах работодатель фиксирует важные для рабочего процесса	**Internal regulation** The documents regulating work in the company. The employer defines rules and standards important for the work process in these documents.

нормы и правила.	
Процессный подход Подход к организации и анализу деятельности компании, основанный на выделении и рассмотрении ее бизнес-процессов, каждый из которых протекает во взаимосвязи с другими бизнес-процессами компании или внешней средой.	**Process approach** Approach to organization and analysis of the company's business based on extraction and review of its business processes each of which is interrelated to the other business processes of the company or external environment.
Руководство Компании Должностные лица Компании, выполняющие управленческие функциии/или имеющие полномочия на принятие управленческих решений в отношении ООО «ЛЕНТА», ее Структурных подразделений или дочерних организаций в соответствии с учредительными документами, организационно распорядительными документами, договорами и/или выданными доверенностями.	**Company's Management** The Company's officials performing management functions and/or authorized for taking management decisions as to Lenta LLC, its structural divisions and subsidiaries in accordance with constituent documents, organizational and administrative documents, contracts and/or issued powers of attorney.
Риск информационной безопасности (Риск ИБ) Это вероятность возникновения негативного события, которое нанесет ущерб организации или физическому лицу.	**Information security risk** Probability of a negative event which incurs damages to the enterprise or the individual.
Система управления информационной безопасности (СУИБ) Совокупность организационных, процедурных, правовых, технических мер и персонала, объединенных на основе заданной модели менеджмента ИБ стандартов серии ISO/IEC 27000.	**Information security management system** Set of organizational, procedural, legal, technical measures and HR united based on a set information security management model by standards ISO/IEC 27000.
Управление информационной безопасности(УИБ) Структурное подразделение в составе Дирекции по обеспечению бизнеса в зоне ответственности которого находится обеспечение информационной безопасности компании.	**Information Security Management** Structural unit under Business Support responsible for the Company's information security.