Одобрено решением Правления
АО «Евразийский Капитал»
Протокол № 21 от «26» августа 2024 года

Утверждено решением СД
АО «Евразийский Капитал»
Протокол № 22 от «29» августа 2024 года

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО «ЕВРАЗИЙСКИЙ КАПИТАЛ»

Алматы 2024

Глава 1. Введение

1. Учитывая тенденции развития мировой и отечественной экономики, в соответствии с которыми, информация и информационные технологии становятся важнейшими активами современного бизнеса, способствующими повышению его конкурентоспособности, Акционерное Общество "Евразийский Капитал" (далее — АО «Евразийский Капитал», Компания), под руководством Совета Директоров, Правления и Председателя Правления (далее — Руководство Компании), уделяет особое внимание решению задачи обеспечения информационной безопасности.
2. Под информационной безопасностью Компания понимает состояние защищенности своих интересов (целей) от угроз в информационной сфере. Защищенность достигается обеспечением совокупности свойств информационных активов: конфиденциальности, целостности и доступности.
3. Информационные ресурсы составляют актив Компании. Случайные или преднамеренные воздействия на информационные ресурсы, т.е. на содержание информации, её носители, процессы обработки и передачи информации могут повлечь для Компании негативные последствия.
4. Политика информационной безопасности АО «Евразийский Капитал» (далее — Политика ИБ, Политика), определяет цели, задачи и принципы Компании в области обеспечения безопасности информационных ресурсов. Политика ИБ распространяется на все информационные ресурсы, владельцем и пользователем которых является Компания. Методы и средства информационной безопасности решают задачу обеспечения безопасности информационных ресурсов при их совместном использовании в бизнес-процессах Компании.
5. Положения настоящей Политики направлены на определение адекватных мер и технологий защиты информационных ресурсов Компании от возможного нанесения им ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи.
6. Политика является общедоступным документом, который может предоставляться без ограничений всем заинтересованным сторонам. Доступ к ссылочным документам Политики может быть ограничен.

Глава 2. Обозначения и сокращения

АРМ	Автоматизированное рабочее место
ИБ	Информационная безопасность
ИР	Информационный ресурс
ИС	Информационная система
ИТ	Информационные технологии
НСД	Несанкционированный доступ
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
СУИБ	Система управления информационной безопасностью

Глава 3. Термины и определения

7. **Аутентификация** — проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.
8. **Безопасность информации** — защищённость информации от её нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного её тиражирования.
9. **Бизнес-процесс** — последовательность технологически связанных операций по предоставлению продуктов, услуг и/или осуществлению конкретного вида деятельности Компании.
10. **Документ** — зафиксированная на материальном носителе информация с реквизитами, позволяющими её идентифицировать.
11. **Доступность информации** -— состояние, характеризуемое способностью ИС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.
12. **Защита информации** — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию и нарушения ее доступности.
13. **Идентификация** - присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.
14. **Информация** — сведения (сообщения, данные) независимо от формы их представления.
15. **Информационная безопасность (ИБ)** — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.
16. **Информационная система (ИС)** — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
17. **Информационный ресурс (актив)** — информация, имеющая ценность и находящаяся в распоряжении Компании.
18. **Инцидент информационной безопасности** — нежелательное или неожиданное событие ИБ, имеющее значительную вероятность нарушения бизнес-процессов или представляющих угрозу ИБ.
19. **Контролируемая зона** — пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств.
20. **Конфиденциальная информация** — информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Республики Казахстан, или по решению ее владельца.
21. **Несанкционированный доступ** — доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.
22. **Риск** — мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

23. **Система управления информационной безопасностью (СУИБ)** — система, предназначенная для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ, основанная на оценке рисков.

24. **Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения** — субъект, в полном объёме реализующий полномочия владения, пользования, распоряжения указанными объектами.

25. **Событие информационной безопасности** — идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности.

26. **Угроза информационной безопасности (ИБ)** — совокупность условий и факторов, создающих опасность нарушения информационной безопасности, приводящую к возможности потерь (ущерба).

27. **Целостность информации** -— устойчивость информации к преднамеренному или случайному воздействию на неё в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

Глава 4. Цели и принципы информационной безопасности

28. Важнейшими целями Компании в области информационной безопасности являются:

- повышение конкурентоспособности бизнеса Компании;
- соответствие требованиям законодательства и договорным обязательствам в части информационной безопасности;
- повышение деловой репутации и корпоративной культуры Компании;
- достижение адекватности мер по защите от угроз информационной безопасности;
- предотвращение и/или снижение ущерба от реализации угроз информационной безопасности.

29. При достижении поставленных целей Компания намерена руководствоваться следующими принципами:

- **Безусловное участие руководства Компании в процессе обеспечения информационной безопасности.** Деятельность по обеспечению информационной безопасности инициирована и контролируется руководством Компании. Руководство Компании выполняет те же правила по обеспечению информационной безопасности, что и все работники Компании.
- **Законность обеспечения информационной безопасности**. Компания реализует меры обеспечения информационной безопасности в строгом соответствии с действующим законодательством и договорными обязательствами.
- **Согласованность действий по обеспечению информационной, физической и экономической безопасности.** Действия по обеспечению информационной, физической и экономической безопасности осуществляются на основе четкого взаимодействия заинтересованных подразделений Компании и согласованы между собой по целям, задачам, принципам, методам и средствам.
- **Экономическая целесообразность.** Компания стремится выбирать меры обеспечения информационной безопасности с учетом затрат на их реализацию, вероятности возникновения угроз информационной безопасности и объема возможных потерь от их реализации.
- **Знание своих работников**. Компания стремится тщательно подбирать персонал (работников), вырабатывать и поддерживать корпоративную этику, что создает

благоприятную среду для деятельности Компании и снижает риски информационной безопасности.

- **Документированность требований информационной безопасности.** Компания стремится, чтобы все требования в области информационной безопасности были зафиксированы во внутренних нормативных документах, утвержденных руководством Компании.
- **Осведомленность в вопросах обеспечения информационной безопасности.** Документированные требования в области информационной безопасности доводятся до сведения работников Компании и контрагентов в части их касающейся. Компания на периодической основе осуществляет информирование, обучение и аттестацию работников по вопросам обеспечения информационной безопасности.
- **Реагирование на инциденты информационной безопасности.** Компания стремится выявлять, учитывать и оперативно реагировать на действительные, предпринимаемые и вероятные нарушения информационной безопасности.
- **Персональная ответственность.** Работники Компании несут персональную ответственность за соблюдение требований информационной безопасности. Обязанности по обеспечению информационной безопасности включаются в трудовые договоры и должностные инструкции работников, а также в договоры (соглашения) с контрагентами.
- **Учет действий с информационными активами.** Компания стремится вести учет всех действий работников Компании и контрагентов с информационными активами Компании.
- **Предоставление минимально необходимых прав доступа.** Работникам Компании и контрагентов предоставляются минимально необходимые права доступа для качественного и своевременного выполнения трудовых обязанностей и договорных обязательств. При этом Компания стремится предоставлять права доступа таким образом, чтобы выполнение особо важной (критичной) операции осуществлялось с участием как минимум двух работников.
- **Учет требований информационной безопасности в проектной деятельности.** Помимо операционной деятельности, Компания стремится учитывать требования информационной — безопасности в проектной — деятельности. Разработка и документирование требований по обеспечению информационной безопасности осуществляется на начальных этапах реализации проектов, связанных с обработкой, хранением и передачей информации.

Глава 5. Основания для разработки

30. Настоящая Политика разработана на основе требований законодательства Республики Казахстан, накопленного в Компании опыта в области обеспечения ИБ, интересов и целей Компании.

31. При написании отдельных положений настоящей Политики использовались следующие нормативные документы:

- СТ РК ISO/IEC 27002-2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью »;
- СТ РК ИСО/МЭК 17799-2006 «Информационная технология. Методы обеспечения защиты».

Глава 6. Область действия

32. Настоящая Политика распространяется на все бизнес-процессы Компании, которые реализуются с использованием информационных технологий, и обязательна для

применения всеми сотрудниками и руководством Компании, а также пользователями информационных ресурсов Компании.

33. Разработка внутренних документов Компании в части вопросов информационной безопасности должна соответствовать настоящей Политике.

34. Лица, осуществляющие разработку внутренних документов Компании, регламентирующих вопросы информационной безопасности, и лица, проводящие организационные и технические мероприятия, связанные с обеспечением информационной безопасности, обязаны руководствоваться настоящей Политикой.

35. Настоящая Политика также должна применяться при взаимодействии и обмене информацией при выполнении договорных обязательств с партнерами и клиентами Компании.

Глава 7. Содержание политики

7.1. Управление информационной безопасностью

36. Для достижения целей Политики и решения задач по защите информации в Компании действует система управления информационной безопасностью, как часть общей системы управления Компании.

37. Система управления информационной безопасностью документируется в правилах, процедурах, рабочих инструкциях. Указанные документы являются обязательными для исполнения всеми работниками Компании в части касающейся. Необходимые требования по информационной безопасности доводятся до сведения работников Компании, в том числе доводятся до сведения изменения при их внесении в документы и требования.

38. Решения о внедрении средств и систем защиты информации принимаются с учетом оценки рисков информационной безопасности и возможного ущерба при реализации угроз.

39. Вопросы непосредственной организации и обеспечения эффективного решения задач информационной безопасности возлагаются руководством на ответственные подразделения Компании. Указанные вопросы отражаются в положениях о подразделениях, должностных инструкциях.

40. По согласованию с руководством Компании в число задач, решаемых подразделением в области информационной безопасности, могут включаться:

- определение требований к защите информации;
- выбор и внедрение средств защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства;
- координация работ подразделений по вопросам комплексной защиты информации;
- контроль и оценка эффективности принятых мер и применяемых средств защиты.

41. Для решения задач, возложенных на подразделения в части информационной безопасности, уполномоченные сотрудники подразделений имеют права:

- контролировать деятельность пользователей по вопросам обеспечения ИБ;
- участвовать в испытаниях разработанных информационных технологий по вопросам оценки качества реализации требований по обеспечению безопасности информации.

7.2. Объект защиты

7.2.1. Информационные ресурсы

42. Защита информации в Компании реализуется на основе определения всех имеющихся информационных ресурсов и последующей оценкой информационных

ресурсов сточки зрения их важности. Принимаемые меры по защите информации должны соответствовать ценности и важности информационных ресурсов.

43. В ИС Компании присутствуют следующие типы ресурсов:

- информационные ресурсы, содержащие конфиденциальную информацию, и/или сведения ограниченного доступа, в том числе информацию о финансовой деятельности Компании;
- открыто распространяемая информация, необходимая для работы Компании, независимо от формы и вида её представления;
- информационные ресурсы, являющиеся результатом интеллектуальной деятельности Компании и принадлежащие Компании на правах интеллектуальной собственности;
- информационная инфраструктура, включая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

44. Для каждого ресурса должен быть назначен владелец (структурное подразделение Компании), который отвечает за соответствующую классификацию информации и ресурсов, и согласует назначение и проверку прав доступа к ресурсам и привилегий.

7.2.2. Классификация информации

45. Все информационные ресурсы, подлежащие защите, должны быть классифицированы в соответствии с важностью и степенью доступа. Классификация информации должна быть документирована и утверждена руководством Компании.

46. Классификация информации должна проводиться владельцем ресурса, хранящего или обрабатывающего информацию, для определения категории ресурса. Периодически классификация должна пересматриваться для поддержания актуальности её соответствия с категорией ресурса.

47. Ресурсы, содержащие конфиденциальную или критичную информацию, могут иметь соответствующую пометку (гриф).

7.3. Оценка и обработка рисков

48. В Компании требования к обеспечению безопасности информационных ресурсов должны формироваться на основе оценки рисков ИБ. Оценка риска ИБ осуществляется на основании мнения экспертов (опытных сотрудников) Компании.

49. Оценка рисков и выбор механизмов контроля рисков должны производиться периодически в целях:

- учета изменений бизнес-требований и приоритетов;
- анализа угроз появления новых уязвимостей в технологиях защиты информации;
- проверки сохранения эффективности реализованных мер обеспечения ИБ.

50. Обработка каждого риска Компании должна осуществляться по критериям для определения возможности принятия риска как допустимого. Риск может быть принят как допустимый, если его последствия достаточно малы, а стоимость нейтрализации не рентабельна для Компании.

51. Для каждого из оцененных рисков должно приниматься одно из решений по его обработке:

- применение механизмов контроля для уменьшения величины риска до приемлемого уровня;
- сознательное и объективное принятие риска как допустимого;
- нейтрализация рисков путём недопущения действий, могущих быть его причиной.

7.4. Ответственность персонала

52. Ответственность за соблюдение установленных правил работы с информационными ресурсами, включая соблюдение правил обеспечения информационной безопасности, должны быть доведены до сотрудника при трудоустройстве и внесены в его должностные обязанности. Сюда должны входить как общие обязанности по реализации и поддержке Политики ИБ, так и конкретные обязанности по защите ресурсов и по соблюдению требований внутренних нормативных документов, связанных с безопасностью.

7.4.1. Условия найма

53. В трудовых договорах, подписываемых всеми принимаемыми на работу сотрудниками, должна быть установлена их ответственность за соблюдение требований ИБ. В трудовой договор должно быть включено согласие сотрудника на проведение контрольных мероприятий со стороны Компании по проверке выполнения требований ИБ.
54. В трудовых договорах, подписываемых всеми принимаемыми на работу сотрудниками, должны быть установлены их обязательства по неразглашению конфиденциальной информации.
55. В договоре должны быть описаны меры, которые будут приняты в случае несоблюдения сотрудником требований ИБ.
56. Обязанности по обеспечению ИБ в части касающейся должны быть включены в должностные инструкции каждого сотрудника Компании.
57. Все принимаемые сотрудники должны быть ознакомлены под роспись с перечнем информации, ограниченного доступа, с установленным режимом с ней и с мерами ответственности за нарушение этого режима.
58. При предоставлении сотруднику доступа к ИС Компании он должен быть проинструктирован в качестве пользователя ИС.

7.4.2. Ответственность руководства

59. Руководство Компании контролирует выполнение правил ИБ всеми сотрудниками в соответствии с установленными в Компании политиками и процедурами.
60. Уполномоченные руководством Компании сотрудники имеют право производить проверки:
- Выполнения действующих инструкций по вопросам ИБ;
- Данных, находящихся на носителях информации;
- Порядка использования сотрудниками информационных ресурсов;
- Содержания служебной переписки.

7.4.3. Обучение ИБ

61. Компания определяет необходимость проведения периодической подготовки сотрудников в области средств и технологий ИБ, принятых в Компании.

7.4.4. Завершение или изменения трудовых отношений

62. При увольнении все предоставленные сотруднику права доступа к ресурсам ИС должны быть удалены.
63. При изменении трудовых отношений удаляются только те права, необходимость в которых отсутствует в новых отношениях.

7.5. Физическая безопасность информационных ресурсов и технических средств

64. Средства обработки информации, поддерживающие критически важные информационные ресурсы Компании, должны быть размещены в защищённых помещениях, расположенных в контролируемой зоне. Такими средствами, как правило являются: серверы, телекоммуникационное оборудование, телефонные станции, кроссовые панели, оборудование, обеспечивающее обработку и хранение конфиденциальной информации.
65. Защищённые помещения должны обеспечиваться соответствующими средствами контроля доступа, обеспечивающими возможность доступа только авторизованного персонала.
66. Вспомогательные технические службы, такие как электропитание, водоснабжение, канализация, отопление, вентиляция и кондиционирование воздуха должны обеспечивать гарантированную и устойчивую работоспособность компонентов ИС Компании.
67. Для хранения служебных документов и машинных носителей с защищаемой информацией помещения, в которых хранятся такие документы, снабжаются сейфами, металлическими шкафами или шкафами, оборудованными замком, а также средствами уничтожения документов на бумажных носителях и уничтожения оптических дисков.
68. В случае утилизации оборудования со всех носителей информации, которыми укомплектовано оборудование, должны гарантированно удаляться все конфиденциальные данные.

7.6. Контроль доступа и управление правами доступа

69. Уровень полномочий каждого сотрудника Компании определяется с учетом его обязанностей. Уровень полномочий каждого пользователя определяется индивидуально. Должно быть обеспечено использование каждым сотрудником только предписанных ему прав по отношению к информации, с которой ему необходимо работать в соответствии с должностными обязанностями.
70. Допуск пользователей к работе с информационными ресурсами должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться в установленном порядке, согласно регламента предоставления доступа пользователей.
71. Доступ сотрудника к информационным ресурсам Компании должен быть санкционирован руководителем структурного подразделения, в котором числится согласно штатному расписанию данный сотрудник, и владельцами соответствующих информационных ресурсов.
72. Для идентификации и аутентификации пользователей при доступе к информационным ресурсам могут использоваться пароли, а также технологии на основе биометрии, сертификатов и аппаратных средств (смарт-карты, e-Token, чипы и т.п.). При использовании паролей должен выполняться набор требований, обеспечивающих необходимый уровень защиты паролей от компрометации.

73. Организация ресурсов локальной сети Компании, включая каталоги и файлы, к которым предоставляется доступ сотрудникам Компании, и их поддержка, регламентируются отдельными внутренними документами.

7.7. Политика работы с информационными системами

74. Ответственность по установке и поддержке вычислительного оборудования и программного обеспечения всех информационных систем, функционирующих в Компании, осуществляется уполномоченным подразделением.
75. Комплектация персональных компьютеров аппаратными и программными средствами, расположение и сетевое подключение компьютеров обеспечивается и контролируется уполномоченным подразделением.
76. Все однотипные АРМ, установленные в Компании, должны иметь унифицированный набор прикладных и офисных программ, определенный назначением АРМ в бизнес-процессе Компании.
77. Изменение установленной аппаратной и программной конфигурации АРМ может проводиться только уполномоченным подразделением.
78. Уполномоченное подразделение имеет право осуществлять контроль над установленным на компьютере программным обеспечением, и принимать меры по ограничению возможностей несанкционированной установки программ.
79. Детальные требования по организации работы в ИС Компании, требования и обязанности сотрудников при работе в ИС излагаются в отдельных документах.

7.7.1. Использование электронной почты

80. Электронная почта используется для обмена в рамках ИС Компании и общедоступных сетей информацией в виде электронных сообщений и документов в электронном виде.
81. Функционирование электронной почты обеспечивается оборудованием, каналами связи и иными ресурсами, принадлежащими Компании.
82. Организацией и обеспечением порядка работы электронной почты в Компании занимается специально уполномоченное подразделение.
83. Корпоративная электронная почта Компании предназначена исключительно для использования в служебных целях.
84. Каждый сотрудник Компании получает почтовый адрес в домене Компании. Адрес электронной почты выдаётся при начальной регистрации пользователя.
85. Любые сообщения корпоративной электронной почты могут быть прочитаны, использованы в интересах Компании, либо удалены уполномоченными сотрудниками Компании.

7.7.2. Работа в публичной сети

86. Доступ к публичной сети (Интернет) предоставляется сотрудникам Компании в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.
87. При использовании сети Интернет запрещено публиковать, загружать и распространять материалы, содержащие конфиденциальную информацию, а также информацию, составляющую коммерческую тайну.
88. Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

7.7.3. Удаленная работа с информационными ресурсами

89. Под удаленной работой с информационными ресурсами Компании понимается получение доступа к ИС Компании из внешней сети.
90. Канал связи между ИС Компании и устройством пользователя во внешней сети должен быть защищен сертифицированным средством криптографической защиты информации (СКЗИ).
91. Процедура управления каналом связи должна предоставлять возможность незамедлительного отключения пользователя от ИС Компании.

7.7.4. Защита от вредоносного ПО

92. Локальные и сетевые ресурсы Компании должны систематически проверяться антивирусным программным обеспечением, в частности, должна быть обеспечена защита входящей электронной почты от проникновения вирусов и другого вредоносного ПО.
93. Важные данные и системная конфигурация должны периодически резервироваться, резервные копии храниться в безопасном месте.
94. Сотрудникам предписаны конкретные меры антивирусной безопасности, изложенные в отдельных документах Компании.

7.8. Приобретение, разработка и обслуживание систем

7.8.1. Требования безопасности для информационных систем

95. При описании требований к созданию новых систем или к усовершенствованию существующих необходимо учитывать потребность в средствах обеспечения безопасности. Требования к безопасности и средства защиты должны соответствовать ценности используемых ИР и потенциальному ущербу для Компании в случае сбоя или нарушения безопасности. Основой для анализа требований к безопасности и выбору мер для поддержки безопасности является оценка рисков и управление рисками.
96. Системные требования к ИБ и процессам, обеспечивающим защиту информации, должны быть включены на ранних стадиях проектирования ИС.

7.8.2. Корректная обработка информации

97. Данные, вводимые в прикладные системы, необходимо проверять, чтобы гарантировать их правильность и соответствие поставленной задаче.

7.8.3. Криптографические средства

98. Все используемые Компанией (приобретаемые) СКЗИ должны эксплуатироваться в полном соответствии с эксплуатационной документацией.
99. Управление ключами должно обеспечивать защиту от их компрометации или утраты.
100. Оборудование, используемое для генерации, хранения и архивирования ключей, должно быть физически защищено.
101. Соглашения с внешними поставщиками криптографических услуг (например, удостоверяющими центрами) об уровне предоставляемого сервиса должны охватывать вопросы ответственности, надёжности сервиса и времени реакции при предоставлении сервиса.

102. Криптографические системы и методы следует использовать для защиты конфиденциальной информации в случаях, когда другие средства не обеспечивают адекватной защиты.

7.8.4. Безопасность процесса разработки и обслуживания информационных систем

103.Внесение изменений в ПО ИС Компании должно проводиться только при наличии существенных объективных причин для внесения изменений.

104. До внесения изменений должно проводиться тестирование нового ПО. Тестовые среды и стенды должны быть отключены от рабочих систем во избежание влияния на рабочие системы. В тестовых системах следует избегать использования конфиденциальных данных. В случае же их вынужденного использования необходимо после тестирования конфиденциальные данные удалить.

105. Для сведения к минимуму риска нарушения работоспособности ИС Компании, следует обеспечивать строгий контроль над внесением изменений в ПО. Необходимо руководствоваться официальными правилами внесения изменений. Эти правила должны гарантировать, что процедуры, связанные с безопасностью и соблюдением контроля, не будут нарушены. При внесении изменений доступ к ИС должен предоставляться ИТ-специалистам в минимально необходимом объеме.

7.9. Управление инцидентами информационной безопасности

106.В Компании должна быть разработана процедура уведомления о происшествиях в области ИБ, а также процедура реагирования на такие происшествия, включающая в себя действия, которые должны выполняться уполномоченными сотрудниками при поступлении сообщений о происшествии.

107. Все сотрудники должны быть ознакомлены с процедурой уведомления, а в их обязанности должна входить максимально быстрая передача информации о происшествиях в области ИБ.

108. Отдельно должна быть разработана процедура контроля инцидентов при осуществлении мониторинга систем автоматизированными средствами.

7.10. Управление непрерывностью и восстановлением

109.В Компании реализуются планы и механизмы, направленные на обеспечение и поддержку непрерывности бизнес-процессов. Указанные планы и механизмы направлены на обеспечение возможности в случае прерывания или сбоя критически важных бизнес-процессов в установленные сроки продолжить или восстановить операции и обеспечить требуемый уровень доступности информации.

110. Каждый план поддержки непрерывности бизнеса должен чётко определять условия начала его исполнения и сотрудников, ответственных за выполнение каждого фрагмента плана. При появлении новых требований необходимо внести поправки в принятые планы действия в нештатных ситуациях.

111. Для каждого плана должен быть назначен определённый владелец. Правила действия в нештатных ситуациях, планы ручного аварийного восстановления и планы возобновления деятельности должны находиться в ведении владельцев соответствующих ресурсов или процессов, к которым они имеют отношение.

7.11. Соблюдение требований законодательства

112. Все значимые требования, установленные действующим законодательством, подзаконными актами и договорными отношениями, а также подход Компании к обеспечению соответствия этим требованиям должны быть явным образом определены, документированы и поддерживаться в актуальном состоянии.

113. Необходимо соблюдение регламентированного процесса, предупреждающего нарушение целостности, достоверности и конфиденциальности ИР, содержащих персональные данные, начиная от стадии сбора и ввода данных до их хранения. Персональные данные конкретного сотрудника и процесс их обработки должен быть открытым для этого сотрудника.

114. В Компании должны быть внедрены соответствующие процедуры для обеспечения соблюдения законодательных ограничений, подзаконных актов и контрактных обязательств по использованию материалов, охраняемых авторским правом, а также по использованию лицензионного ПО.

115. Важная документация Компании должна быть защищена от утери, уничтожения и фальсификации в соответствии с требованиями законодательства, подзаконных актов, контрактных обязательств и бизнес-требований.

116. Система хранения и обработки должна обеспечивать чёткую идентификацию записей и их периода хранения в соответствии с требованиями законов и нормативных актов. Эта система должна иметь возможность уничтожения записей по истечении периода хранения, если эти записи больше не требуются Компании.

7.12. Аудит информационной безопасности

117.Компания должна систематически осуществлять:

- контроль текущего уровня защищённости ИС;
- выявление и локализацию уязвимостей в системе защиты ИС;
- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ИР;
- оценку соответствия ИС требованиям настоящей Политики;
- выработку рекомендаций по совершенствованию СУИБ за счёт внедрения новых и повышения эффективности существующих мер защиты информации.

118. В рамках указанных действий проводятся:

- сбор и анализ исходных данных об организационной и функциональной структуре ИС, необходимых для оценки состояния ИБ;
- анализ существующей политики безопасности и других организационно-распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их разработке (или доработке);
- технико-экономическое обоснование механизмов безопасности;
- проверка правильности подбора и настройки средств защиты информации, формирование предложений по использованию существующих и установке дополнительных средств защиты для повышения уровня надёжности и безопасности ИС;
- разбор инцидентов ИБ и минимизация возможного ущерба от их проявления.

119. Руководство и сотрудники Компании обязаны предоставлять всю необходимую для проведения указанных работ информацию.

Глава 8. Ответственность

120. Приоритетные направления деятельности в области обеспечения ИБ, меры по реализации настоящей Политики списки объектов и сведений, подлежащих защите,

утверждает руководитель Компании. Руководитель Компании также осуществляет общее руководство обеспечением ИБ.

121. Все руководители структурных подразделений несут прямую ответственность за реализацию Политики и её соблюдение персоналом в соответствующих подразделениях.

122. Работники Компании несут персональную ответственность за соблюдение требований документов ИБ в части касающейся.

123. В трудовых договорах и должностных инструкциях работников устанавливается ответственность за сохранность служебной информации, ставшей известной в силу выполнения своих обязанностей. Нарушение требований нормативных актов Компании по обеспечению ИБ является чрезвычайным происшествием и может служить поводом и основанием для проведения расследования.

Глава 9. Контроль и пересмотр

124. Общий контроль состояния ИБ осуществляется руководителем Компании.

125. Текущий контроль соблюдения настоящей Политики осуществляется подразделениями Компании в рамках, определенных положениями о подразделениях и должностными инструкциями, а также в рамках иных контрольных мероприятий.

126. Изменения и дополнения в настоящую Политику утверждаются руководителем Компании в форме новой редакции Политики.

Лист ознакомления с «Политикой информационной безопасности АО «Евразийский Капитал»

№	Ф.И.О.	Должность/Наименование структурного подразделения	Подпись	Дата
1	Айтқожа Асқар Айғожаұлы	Председатель Правления		
2	Омарханова Гульнур Еркенбековна	Директор Департамента управления инвестиционным портфелем / Член Правления		
3	Каташева Айнагуль Исановна	Главный бухгалтер – Директор Департамента бухгалтерского учета и отчетности		
4	Али Исламбек Серікбайұлы	Директор Торгового департамента		
5	Алибаева Куралай Сагатхановна	Директор Департамента Бэк-офис		
6	Свиридова Ольга Владимировна	Директор Юридического департамента / Член Правления		
7	Мусабекова Айгуль Рустембековна	Юрист Юридического департамента		
8	Калижаров Адиль Кабдрахманович	Начальник Службы управления рисками		
9	Сагындыков Али Аскарович	Аналитик Аналитического отдела Департамента управления инвестиционным портфелем		
10	Калиаскарова Назира Амановна	Заместитель Главного бухгалтера Департамента бухгалтерского учета и отчетности		
11	Муканова Айгерим Сериккызы	Главный специалист Департамента Бэк-офис		
12	Дәулетқызы Дана	Специалист Департамента Бэк-офис		
13	Бухтин Евгений Александрович	Специалист Департамента информационного обеспечения		
14	Нурмухамедова Меруерт Кабуловна	Внутренний аудитор Службы внутреннего аудита		
15	Сагитжан Самал Ержановна	Заместитель Директора Торгового департамента		
16	Бафин Таттимбет Балхашевич	Специалист по финансовому мониторингу Службы управления рисками		
17	Хасенова Гульнара Сериковна	Главный специалист Департамента управления инвестиционным портфелем		
18	Субханбердин Мади Сержанұлы	Трейдер Торгового департамента		

19	Алимов Динислам Сарсенбаевич	Старший Трейдер Торгового департамента		
20	Кульшуманова Айдана Альбековна	Специалист Департамента продаж и работы с клиентами		
21	Абдумуталова Сабина Талгаткызы	Офис-менеджер Административной службы		