НАО «Костанайский региональный университет имени Ахмет Байтұрсынұлы»

BAITURSYNULY UNIVERSITY

Утверждаю
Председатель Правления – Ректор
_____ С.Куанышбаев
16.06.2026 г.

ПРАВИЛА

ПРОВЕДЕНИЕ ВНУТРЕННЕГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПР 015-2026

Костанай

Предисловие

1 РАЗРАБОТАНЫ отделом разработки и сопровождения программного обеспечения

2 ВНЕСЕНЫ отделом разработки и сопровождения программного обеспечения

3 УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ: приказом Председателя Правления - Ректора от 16. 06. 2026 года № 213 ОД

4 РАЗРАБОТЧИК:
В. Гриднева – начальник отдела разработки и сопровождения программного обеспечения

5 ЭКСПЕРТЫ:
Ж.Жарлыгасов – проректор по исследованиям, инновациям и цифровизации, кандидат сельскохозяйственных наук;
А.Шмит – начальник отдела технического обеспечения

6 ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 3 года

7 ВВЕДЕНЫ впервые

Содержание

Глава 1. Область применения

1. Настоящие Правила проведения внутреннего аудита информационной безопасности (далее – Правила) определяют порядок организации и проведения внутреннего аудита информационной безопасности в НАО «Костанайский региональный университет имени Ахмет Байтұрсынұлы» (далее – Университет).

2. Правила разработаны в целях осуществления внутреннего контроля состояния информационной безопасности, соблюдения требований локальных нормативных документов Университета, выявления уязвимостей, недостатков организационных и технических мер защиты информации, а также выработки рекомендаций по повышению уровня защищенности электронных информационных ресурсов, информационных систем и активов Университета.

3. Внутренний аудит информационной безопасности проводится сотрудниками Университета и распространяется на электронные информационные ресурсы, информационные системы, серверное оборудование, рабочие станции, сетевую инфраструктуру, программное обеспечение, корпоративные сервисы и иные активы, связанные со средствами обработки информации.

4. Внутренний аудит информационной безопасности включает:

1) проверку соблюдения требований локальных нормативных документов по ИБ;

2) анализ состояния организационных и технических мер защиты информации;

3) выявление уязвимостей и потенциальных угроз ИБ;

4) проверку корректности разграничения прав доступа;

5) проверку состояния резервного копирования и восстановления информации;

6) проверку антивирусной защиты;

7) анализ журналов событий и инцидентов ИБ;

8) оценку соблюдения правил использования сети Интернет и корпоративной электронной почты;

9) выработку рекомендаций по устранению выявленных нарушений.

5. Правила входят в состав нормативно-справочной документации Университета, являются обязательными для исполнения всеми сотрудниками Университета, а также доводятся до сведения иных третьих лиц, участвующих в эксплуатации и обслуживании средств обработки информации Университета.

Глава 2. Нормативные ссылки

6. В настоящих Правилах использованы ссылки на следующие нормативные документы:

1) Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»;

2) Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»;

3) Устав НАО «Костанайский региональный Университет имени Ахмет Байтұрсынұлы», утвержденный приказом Председателя Комитета государственного имущества и приватизации Министерства финансов Республики Казахстан от 05 июня 2020 года № 350 с изменениями от 03.10.2023г.;

4) СО 002-2025 Стандарт организации. Делопроизводство;

5) ДП 001-2025 Документированная процедура. Управление документацией;

6) П 054-2024 Политика информационной безопасности НАО «Костанайский региональный университет имени Ахмет Байтұрсынұлы»;

Глава 3. Определения

7. В настоящих Правилах применяются следующие определения:

1) внутренний аудит информационной безопасности – процесс внутренней проверки состояния информационной безопасности Университета, направленный на оценку соблюдения требований локальных нормативных документов и эффективности мер защиты информации;

2) актив, связанный со средствами обработки информации (далее – актив ИБ) — материальный или нематериальный объект, который является информацией, содержит информацию либо используется для обработки, хранения или передачи информации и имеет ценность для Университета;

3) информационная безопасность – состояние защищенности электронных информационных ресурсов, информационных систем и активов ИБ Университета от внутренних и внешних угроз;

4) информационная система – под информационными системами в настоящих Правилах понимаются все информационные системы, корпоративные сервисы и веб-ресурсы Университета, используемые для обработки, хранения и передачи информации;

5) инцидент информационной безопасности – событие или действие, создающее угрозу конфиденциальности, целостности или доступности информации;

6) уязвимость – недостаток организационных, программных, технических или физических мер защиты, который может быть использован для реализации угрозы ИБ;

7) аудиторская группа – сотрудники Университета, назначенные для проведения внутреннего аудита информационной безопасности.

Глава 4. Обозначения и сокращения

8. В настоящей документированной процедуре применяются следующие сокращения:

1) ДП – документированная процедура;
2) НАО – Некоммерческое акционерное общество;
3) ОДО – отдел документационного обеспечения;
4) СО – стандарт организации;
5) ИБ – информационная безопасность;
6) ИС – информационная система;
7) П – положение;
8) ПР – правила;
9) LMS – система управления обучением (Learning Management System);
10) CMS – система управления контентом (Content Management System).

Глава 5. Основные цели и задачи

9. Основными целями внутреннего аудита ИБ являются:
1) оценка текущего состояния ИБ Университета;
2) контроль соблюдения требований локальных нормативных документов по ИБ;
3) выявление уязвимостей и недостатков системы защиты информации;
4) анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС;
5) повышение устойчивости информационных систем и корпоративных сервисов Университета.
10. Основными задачами внутреннего аудита являются:
1) проверка соблюдения требований по разграничению прав доступа;
2) проверка соблюдения требований антивирусного контроля;
3) проверка состояния резервного копирования и восстановления информации;
4) анализ журналов событий и инцидентов ИБ;
5) проверка актуальности обновлений программного обеспечения;
6) проверка соблюдения правил использования сети Интернет и корпоративной электронной почты;
7) проверка соблюдения требований физической защиты серверного и сетевого оборудования;
8) оценка выполнения мероприятий по снижению рисков информационной безопасности;
9) подготовка рекомендаций по устранению выявленных нарушений.

Глава 6. Виды внутреннего аудита информационной безопасности

11. Внутренний аудит информационной безопасности подразделяется на:
1) плановый аудит;
2) внеплановый аудит.
12. Плановый аудит проводится в соответствии с ежегодным планом-

графиком внутреннего аудита информационной безопасности, который составляется сотрудниками, ответственными за обеспечение ИБ Университета, и утверждается руководством Университета. Форма плана-графика внутреннего аудита ИБ приведена в Приложении А к настоящим Правилам.

13. Внеплановый аудит проводится:

1) при возникновении инцидентов ИБ;
2) при выявлении признаков нарушения требований ИБ;
3) после внедрения новых ИС, сервисов или технических средств;
4) по поручению руководства Университета.

14. В зависимости от целей и задач внутренний аудит информационной безопасности может включать:

1) аудит ИС, корпоративной вычислительной сети, серверного, сетевого и иного оборудования в целях оценки состояния ИБ и подготовки рекомендаций по совершенствованию мер защиты информации;

2) профилактический аудит, направленный на обеспечение соответствия системы ИБ требованиям законодательства Республики Казахстан и внутренним нормативным документам Университета;

3) аудит (служебное расследование), проводимый в целях установления причин и обстоятельств инцидентов информационной безопасности;

4) аудит, проводимый с участием работников структурных подразделений Университета, представителей обслуживающих организаций либо привлеченных специалистов в пределах их компетенции и на основании договорных обязательств.

Глава 7. Организация и порядок проведения внутреннего аудита информационной безопасности

15. Проведение внутреннего аудита осуществляется сотрудниками отдела разработки и сопровождения программного обеспечения, отдела технического обеспечения и сотрудниками, ответственными за обеспечение информационной безопасности.

16. Для проведения аудита назначаются аудиторская группа и ее руководитель.

17. При проведении аудита учитываются:

1) цели и область аудита;
2) перечень проверяемых информационных систем и активов ИБ;
3) сроки проведения аудита;
4) перечень применяемых нормативных документов;
5) результаты предыдущих проверок и инцидентов ИБ.

18. На основании утвержденного плана-графика внутреннего аудита ИБ, составленного по форме согласно Приложению А к настоящим Правилам, формируется программа проведения конкретного аудита. Форма программы внутреннего аудита ИБ приведена в Приложении Б к настоящим Правилам.

19. Подготовка к проведению аудита включает:

1) изучение локальных нормативных документов;

2) анализ журналов событий и инцидентов;

3) определение критериев аудита;

4) определение перечня проверяемых активов ИБ;

5) подготовку проверяемых вопросов, включаемых в программу внутреннего аудита информационной безопасности по форме согласно Приложению Б к настоящим Правилам.

20. Руководитель аудиторской группы знакомит с программой аудита всех членов аудиторской группы. После этого, не менее чем за 7 календарных дней до проведения аудита, программа аудита передается руководителям проверяемых структурных подразделений для согласования условий и времени проведения аудита. Согласованная программа аудита передается на утверждение руководству Университета.

21. В процессе проведения аудита применяются следующие методы:

1) анализ организационно-распорядительной документации;

2) проверка настроек информационных систем и серверного оборудования;

3) анализ журналов событий;

4) интервьюирование сотрудников;

5) проверка соблюдения требований локальных нормативных документов;

6) использование специализированных программных средств мониторинга и анализа.

22. При проведении внутреннего аудита могут проверяться:

1) серверное оборудование;

2) рабочие станции;

3) локальная вычислительная сеть;

4) системы резервного копирования;

5) системы антивирусной защиты;

6) корпоративная электронная почта;

7) LMS, CMS, базы данных и иные информационные системы;

8) журналы регистрации инцидентов ИБ;

9) права доступа пользователей.

23. При проведении внутреннего аудита ИБ члены аудиторской группы имеют право на:

1) доступ в служебные, серверные, коммутационные, аппаратные и иные помещения Университета, содержащие активы ИБ либо используемые для размещения и прохождения линий связи и сетевых коммуникаций, необходимых для проведения аудита;

2) доступ к информационным системам, корпоративной вычислительной сети, серверам, сетевому оборудованию, системам видеонаблюдения, интернет-ресурсам и документации, относящимся к предмету аудита, в пределах предоставленных полномочий;

3) запрос и получение необходимых документов, сведений, журналов учета, отчетов, логов и иных материалов, относящихся к предмету аудита;

4) получение информации о событиях и записях, содержащихся в ИС, журналах регистрации событий, средствах мониторинга и иных системах контроля, в пределах, установленных законодательством Республики Казахстан и внутренними документами Университета;

5) получение от работников структурных подразделений устных и письменных пояснений по вопросам, возникающим в ходе проведения аудита;

6) привлечение при необходимости работников структурных подразделений, а также представителей обслуживающих организаций и поставщиков ИС по согласованию с руководством Университета.

24. По результатам аудита составляется отчет о внутреннем аудите ИБ по форме согласно Приложению В к настоящим Правилам.

25. Отчет о внутреннем аудите ИБ содержит:

1) объект аудита;
2) дату проведения аудита;
3) перечень выявленных нарушений;
4) выявленные уязвимости;
5) оценку уровня защищенности;
6) рекомендации по устранению нарушений;
7) сроки устранения выявленных недостатков;
8) состав аудиторской группы;
9) ответственных исполнителей;
10) заключение по результатам аудита.

Глава 8. Корректирующие мероприятия

26. По результатам внутреннего аудита разрабатываются корректирующие мероприятия по устранению выявленных нарушений и снижению рисков ИБ.

27. Корректирующие мероприятия могут включать:

1) изменение прав доступа пользователей;
2) обновление программного обеспечения;
3) усиление антивирусной защиты;
4) корректировку параметров безопасности;
5) обновление конфигурации серверов и сетевого оборудования;
6) восстановление или проверку работоспособности резервных копий;
7) ремонт, замену, модернизацию или приобретение серверного, сетевого, компьютерного оборудования, программного обеспечения и средств защиты информации в установленном порядке;
8) проведение дополнительного обучения сотрудников.

28. Корректирующие мероприятия, сроки их выполнения и ответственные исполнители отражаются в отчете о внутреннем аудите ИБ по форме согласно Приложению В к настоящим Правилам.

29. Ответственные исполнители, указанные в корректирующих мероприятиях отчета о внутреннем аудите ИБ, обеспечивают выполнение мероприятий в установленные сроки. По результатам выполнения корректирующих мероприятий ответственные исполнители представляют служебную записку о выполнении мероприятий сотрудникам, ответственным за обеспечение ИБ.

30. Сотрудники, ответственные за обеспечение ИБ, осуществляют контроль выполнения корректирующих мероприятий. При необходимости проводится контрольная проверка либо повторный внутренний аудит устранения выявленных несоответствий.

Глава 9. Ответственность

31. Сотрудники Университета обязаны предоставлять информацию и содействовать проведению внутреннего аудита ИБ в пределах своих должностных обязанностей.

32. Руководитель аудиторской группы несет ответственность за:

1) организацию проведения внутреннего аудита;
2) объективность результатов проверки;
3) достоверность оформляемых материалов;
4) своевременное предоставление отчетов.

33. Руководители структурных подразделений несут ответственность за устранение выявленных нарушений в установленные сроки.

34. Сотрудники, ответственные за обеспечение ИБ, осуществляют контроль выполнения мероприятий по устранению нарушений и снижению рисков информационной безопасности.

Глава 10. Порядок внесения изменений

35. Внесение изменений в настоящие Правила осуществляется по инициативе начальника отдела разработки и сопровождения программного обеспечения, начальника отдела технического обеспечения, проректора по исследованиям, инновациям и цифровизации в соответствии с ДП 001-2025 Документированная процедура. Управление документацией.

Глава 11. Согласование, хранение и рассылка

36. Согласование и рассылка Правил производятся в соответствии с ДП 001-2025 Документированная процедура. Управление документацией.

37. Настоящие Правила согласовываются с проректором по исследованиям, инновациям и цифровизации, начальником отдела правового обеспечения и государственных закупок, начальником отдела управления персоналом и начальником отдела документационного обеспечения.

38. Подлинник настоящих Правил вместе с «Листом согласования» передается на хранение в ОДО по акту приема-передачи.

39. Рабочий экземпляр настоящих Правил размещается на сайте Университета с доступом из внутренней корпоративной сети.

Приложение А

Образец плана-графика внутренних аудитов информационной безопасности

План-график внутренних аудитов информационной безопасности
на _____ год

№	Объект аудита (примеры)	Дата предыдущего внутреннего аудита	Плановый срок проведения аудита	Фактическая дата проведения аудита
1	Серверное оборудование			
2	Рабочие станции			
3	Локальная вычислительная сеть			
4	Информационные системы Университета			
5	Корпоративная электронная почта			
6	Система резервного копирования			
7	Антивирусная защита			
8	Права доступа пользователей			
9	Серверные помещения			
10	Журналы инцидентов ИБ и внештатных ситуаций			

Примечание: в случае возникновения инцидентов информационной безопасности, выявления признаков нарушения требований ИБ, внедрения новых информационных систем, сервисов или технических средств проводится внеплановый аудит.

Руководитель аудиторской группы

Должность _____ И.О. Фамилия
(подпись)

Дата составления: «____» _____ 20 __года

Приложение Б

Образец программы внутреннего аудита

НАО «Костанайский региональный университет имени Ахмет Байтұрсынұлы»

Утверждаю
Должность
_____Ф.И.О
_____202 __г.

ПРОГРАММА ВНУТРЕННЕГО АУДИТА ИБ № _____

1. Проверяемое структурное подразделение
2. Объект аудита
3. Основание проведения аудита
4. Цель аудита
5. Задачи аудита
6. Сроки проведения аудита
7. Область аудита
8. Состав аудиторской группы
9. Перечень нормативных документов, на соответствие которым проводится аудит:
10. Критерии аудита:

Критериями аудита являются требования законодательства Республики Казахстан, Политики информационной безопасности Университета и локальных нормативных документов Университета в области информационной безопасности, применимые к объекту аудита.

При проведении внутреннего аудита, в зависимости от цели и области аудита, проверяется соблюдение требований по следующим направлениям:

1) наличие и актуальность нормативно-справочной документации по ИБ;
2) соблюдение требований Политики информационной безопасности;
3) соблюдение требований по идентификации, классификации и маркировке активов;
4) соблюдение требований по оценке рисков информационной безопасности;
5) соблюдение требований по аутентификации и разграничению прав доступа;
6) соблюдение требований антивирусного контроля;
7) соблюдение требований по использованию сети Интернет и корпоративной электронной почты;
8) соблюдение требований по резервному копированию и восстановлению информации;
9) соблюдение порядка реагирования на инциденты ИБ и внештатные ситуации;
10) соблюдение требований физической защиты серверного и сетевого оборудования.

11. Проверяемые вопросы в рамках аудита:

Проверяемые вопросы определяются аудиторской группой с учетом цели, задач, объекта аудита, проверяемого структурного подразделения, используемых информационных систем, оборудования и действующих локальных нормативных документов Университета.

В рамках настоящего аудита могут проверяться следующие вопросы:

1) наличие утвержденных и актуальных документов по информационной безопасности;
2) наличие актуального реестра активов, связанных со средствами обработки информации;
3) наличие ответственных лиц за эксплуатацию информационных систем, сервисов и оборудования;

Продолжение приложения Б

4) порядок предоставления, изменения и аннулирования прав доступа пользователей;
5) соблюдение требований к учетным записям и паролям;
6) своевременность блокировки учетных записей уволенных работников;
7) наличие и актуальность антивирусной защиты на рабочих станциях и серверах;
8) регулярность обновления операционных систем, прикладного программного обеспечения и антивирусных баз;
9) выполнение резервного копирования по установленному графику;
10) наличие журналов резервного копирования и восстановления информации;
11) проведение тестового восстановления данных;
12) ведение журнала регистрации инцидентов ИБ и учета внештатных ситуаций;
13) соблюдение правил использования сети Интернет;
14) соблюдение правил использования корпоративной электронной почты;
15) наличие ограничений физического доступа к серверному и сетевому оборудованию;
16) наличие условий для безопасной эксплуатации серверного оборудования;
17) наличие схемы локальной вычислительной сети;
18) наличие журналов, отчетов, заявок и иных рабочих документов, подтверждающих выполнение процедур ИБ.
19) иные вопросы, относящиеся к цели и области конкретного внутреннего аудита.

12. Методы проведения аудита:

При проведении аудита применяются следующие методы:
1) анализ документов;
2) анализ журналов и отчетов;
3) осмотр оборудования и помещений;
4) проверка настроек информационных систем и сервисов;
5) интервьюирование работников;
6) анализ событий информационной безопасности;
7) использование средств мониторинга и администрирования.

13. Дата представления отчета_____

Руководитель аудиторской группы:

Должность _____ И.О. Фамилия
(подпись)

Аудиторы:

Должность _____ И.О. Фамилия
(подпись)

Должность _____ И.О. Фамилия
(подпись)

Согласовано

Руководитель проверяемого структурного подразделения

Должность _____ И.О. Фамилия
(подпись)

Приложение В

Образец отчета о внутреннем аудите

НАО «Костанайский региональный университет имени Ахмет Байтұрсынұлы»

Утверждаю
Должность
_____Ф.И.О
_____202 __г.

ОТЧЕТ О ВНУТРЕННЕМ АУДИТЕ ИБ № _____

1. Общие сведения

№	Показатель	Сведения
1.	Проверяемое структурное подразделение	
2.	Объект аудита	
3.	Руководитель структурного подразделения	
4.	Руководитель аудиторской группы	
5.	Аудиторы	
6.	Дата проведения аудита	
7.	Основание проведения аудита	
8.	Документы, на соответствие которым проводился аудит	

2. Результаты аудита

№	Показатель	Количество / отметка	Примечание
1	Выявленные несоответствия		
2	Выявленные уязвимости		
3	Предложения и рекомендации		

3. Выявленные несоответствия/уязвимости и корректирующие мероприятия по результатам аудита

1. Несоответствие/уязвимость № 1
В ходе проведения внутреннего аудита ИБ выявлено следующее несоответствие/уязвимость:

_____

_____

Основание / нарушенное требование:

_____

Продолжение приложения В

Рекомендация по устранению:

_____

_____

4. Заключение по результатам аудита

Деятельность _____
наименование подразделения
удовлетворяет / не удовлетворяет установленным требованиям_____

Корректирующие мероприятия (план):

№	Корректирующее мероприятие	Ответственный исполнитель	Срок выполнения
1			
2			
3			

Необходимость повторного внутреннего аудита: ДА / НЕТ.

Предложения и рекомендации

_____

_____

Составил:

Руководитель аудиторской группы:

Должность _____ И.О. Фамилия
(подпись)

Аудиторы:

Должность _____ И.О. Фамилия
(подпись)

Должность _____ И.О. Фамилия
(подпись)

С отчетом ознакомлен:

Руководитель проверяемого структурного подразделения

Должность _____ И.О. Фамилия
(подпись)