Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

И Н С Т Р У К Ц И Я О Р Г А Н И З А Ц И И

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Инструкция по организации контроля эффективности защиты информации в автоматизированных информационных системах

ОРИГИНАЛ

Содержание

УТВЕРЖДЕНА
Приказом ректора
(чем) (должность)

от «14» апреля 2022 г. № 264-О
(дата)

И Н С Т Р У К Ц И Я О Р Г А Н И З А Ц И И
СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Инструкция по организации контроля эффективности защиты информации в автоматизированных информационных системах — Введена впервые

1 Область применения

1.1 Настоящая инструкция по организации контроля эффективности защиты информации в автоматизированных информационных системах, разработана в целях распределения ответственности за контролем соблюдения требований законодательства в сфере защиты персональных данных в федеральном государственном бюджетном образовательном учреждение высшего образования «Иркутский национальный исследовательский технический университет» (далее - ФГБОУ ВО «ИРНИТУ»).

1.2 Требования данной инструкции распространяются на руководителей подразделений, участвующих в обработке персональных данных в ФГБОУ ВО «ИРНИТУ», а также лиц, обслуживающих информационные системы, содержащие персональные данные.

2 Нормативные ссылки

Настоящая инструкция разработана в соответствии и содержит ссылки на следующие нормативные документы:

Конституция Российской Федерации.

Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».

Приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 г. №378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Устав ФГБОУ ВО «ИРНИТУ».

Концепция информационной безопасности автоматизированных информационных систем ФГБОУ ВО «ИРНИТУ».

Политика информационной безопасности автоматизированных информационных систем ФГБОУ ВО «ИРНИТУ».

СТО 002 Система менеджмента качества. Порядок управления документированной информацией (документами) СМК.

3 Термины, определения и сокращения

3.1 В настоящей инструкции применены следующие термины с соответствующими определениями:

Автоматизированная информационная система – информационная система, состоящая из персонала и комплекса средств автоматизации его деятельности.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных), являющемуся абитуриентом или обучающимся ФГБОУ ВО «ИРНИТУ».

Система менеджмента качества – часть системы менеджмента применительно к качеству.

Стандарт организации – нормативный документ по стандартизации, разработанный, как правило, на основе согласия, характеризующегося отсутствием возражений по существенным вопросам у большинства заинтересованных сторон, устанавливающий комплекс норм, правил, требований к различным видам деятельности университета или их результатам и утвержденный приказом руководства университета.

3.2 В настоящей инструкции используются следующие сокращения:

АИС – автоматизированная информационная система;

ПДн – персональные данные;

СМК – система менеджмента качества;

СТО – стандарт организации;

ФГБОУ ВО «ИРНИТУ» – Федеральное государственное бюджетное образовательное учреждение высшего образования «Иркутский национальный исследовательский технический университет».

4 Ответственность

4.1 Ответственность за разработку, пересмотр, идентификацию внесенных изменений в данную инструкцию возложена на начальника отдела информационной безопасности и документооборота ФГБОУ ВО «ИРНИТУ».

4.2 Разработчик настоящей инструкции осуществляет периодическую проверку (пересмотр) данного документа в установленном порядке согласно СТО 002 Система менеджмента качества. Порядок управления документированной информацией (документами) СМК.

4.3 Ответственность за выполнение требований данной инструкции возлагается на руководителей подразделений, участвующих в обработке персональных данных в ФГБОУ ВО «ИРНИТУ», а также лиц, обслуживающих информационные системы, содержащие персональные данные.

5 Общие положения

5.1 Контроль эффективности защиты информации проводится в следующих целях:

a) проверка выполнения требований организационно-распорядительной документации по защите информации в автоматизированной информационной системе;

b) оценка уровня осведомленности и знаний работников ФГБОУ ВО «ИРНИТУ» в области обработки и защиты ПДн в АИС;

c) оценка обоснованности и эффективности применяемых мер и средств защиты АИС.

6 Виды контроля эффективности

6.1 Контроль эффективности осуществляется посредством проведения проверок.

6.2 Проверки соответствия обработки ПДн в АИС установленным требованиям разделяются на следующие виды:

a) регулярные контрольные мероприятия;
b) плановые контрольные мероприятия (далее – внутренняя проверка);
c) внеплановые контрольные мероприятия.

6.3 Регулярные контрольные мероприятия проводятся следующими лицами:

a) начальниками структурных подразделений;
b) начальником отдела информационной безопасности и документооборота;
c) администраторами информационной безопасности;
d) системными администраторами.

6.4 Регулярные контрольные мероприятия проводятся в соответствии с требованиями организационно распорядительной документации и предназначены для осуществления контроля выполнения требований в области защиты ПДн в ФГБОУ ВО «ИРНИТУ».

6.5 Регулярные контрольные мероприятия проводятся в соответствии с «Листом периодичности регулярного контроля соответствия обработки ПДн в АИС требованиям к защите ПДн в АИС» (Приложение 1) и направлены на постоянное совершенствование защиты ПДн, обрабатываемых в АИС. В случае выявления нарушений при проведении контроля, составляется «Акт выявления нарушений в сфере защиты персональных данных» (далее – акт) согласно Приложению 6.

6.6 Плановые контрольные мероприятия осуществляются работниками отдела информационной безопасности и документооборота.

6.7 Плановые контрольные мероприятия проводятся в соответствии с «Листом периодичности внутренних проверок режима обработки и защиты персональных данных в АИС» (Приложение 2).

6.8 Внеплановые контрольные мероприятия проводятся на основании решения ректора, проректора по цифровой трансформации, начальника управления информатизации или начальника отдела информационной безопасности и документооборота ФГБОУ ВО «ИРНИТУ». Внеплановые проверки могут проводиться в следующих случаях:

a) по результатам расследования выявленных нарушений требований законодательства в сфере ПДн;
b) по результатам внешних контрольных мероприятий, проводимых уполномоченным органом по защите прав субъектов ПДн;
c) при существенных изменениях процессов или процедур обработки и защиты ПДн;
d) при выявлении большого числа нарушений требований законодательства в сфере ПДн или повторяемости одних и тех же нарушений от проверки к проверке.

7 Порядок проведения контрольных мероприятий

7.1 Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполняться следующие проверки:

a) порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;
b) эффективность принимаемых мер по обеспечению безопасности персональных данных;
c) соответствие состава и структуры программно-технических средств автоматизированной информационной системы документированному составу и структуре средств, представленному в техническом паспорте автоматизированной информационной системы;
d) порядок и условия применения средств защиты информации;

e) порядок и условия допуска лиц в помещения, где осуществляется обработка персональных данных;

f) порядок организации и правильности учета машинных носителей информации;

g) соблюдение установленных правил доступа субъектов доступа к объектам доступа;

h) наличие (отсутствие) фактов несанкционированного доступа к персональным данным;

i) соблюдение установленных правил организации парольной и антивирусной защиты;

j) знание персоналом базы нормативно-методических документов по защите информации.

k) наличие, учет, порядок хранения и обезличивания персональных данных;

l) соблюдение правил доступа к персональным данным;

m) порядок проведения мероприятий и результаты по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

n) порядок проведения мероприятий по обеспечению целостности персональных данных.

7.2 При проведении проверок работники отдела информационной безопасности и документооборота имеют право:

a) запрашивать у других работников информацию, необходимую для реализации полномочий;

b) требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных;

c) принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

d) привлекать в установленном порядке специалистов, имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе проверки, и выработки соответствующих рекомендаций и заключений;

e) вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

f) вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации о персональных данных.

7.3 По результатам внутренней проверки оформляются следующие документы:

a) протокол проведения внутренней проверки;

b) акт, выявленных нарушений.

Также делается запись в электронном журнале.

7.4 По результатам внутренней проверки составляется «Протокол результатов проведения внутренней проверки обеспечения безопасности информации» (далее – протокол) согласно Приложению 5, результаты проверок фиксируются в электронном журнале. Протокол подписывается работниками отдела информационной безопасности и документооборота, осуществившими проверку.

7.5 Электронный журнал должен содержать информацию: название мероприятия, дата проведения мероприятия, исполнитель, результат приведения мероприятия (с нарушениями/ без нарушений), номер акта, номер протокола.

7.6 При выявлении нарушений в сфере защиты ПДн составляется акт, выявленные нарушения фиксируются в электронном журнале. Акт подписывается сотрудниками, проводившими проверку.

7.7 При выявлении в ходе проверки нарушений, в протоколе делается запись о

мероприятиях по устранению нарушений и сроках исполнения.

7.8 Ответственный за ведение электронного журнала – начальник отдела информационной безопасности и документооборота.

7.9 Протоколы, акты, журнал хранятся в отделе информационной безопасности и документооборота. Уничтожение протоколов и актов проводится начальником отдела информационной безопасности и документооборота самостоятельно в январе года следующего за проверочным годом. При необходимости протоколы могут храниться до полного устранения нарушений.

Приложение 1 Лист периодичности регулярного контроля соответствия обработки персональных данных в автоматизированных информационных системах требованиям к защите персональных данных
(обязательное)

Мероприятие	Периодичность	Исполнитель
Контроль соблюдения режима защиты персональных данных, политики в отношении обработки персональных данных, выполнения работниками обязанностей по защите персональных данных, определенных в организационно-распорядительной документации	Ежедневно	Начальники структурных подразделений
Контроль выполнения требований по режиму доступа в помещения, в которых ведется обработка персональных данных и размещены технические средства, позволяющие осуществлять обработку персональных данных	Ежедневно	
Контроль соблюдения режима обработки персональных данных	Ежедневно	
Контроль целостности средств вычислительной техники, используемых для обработки персональных данных Контроль корректной работы системного и прикладного программного обеспечения, средств защиты информации Контроль состава технических средств	Еженедельно	Администратор информационной безопасности
Контроль выполнения антивирусной защиты, неизменности настроек средств антивирусной защиты и своевременным обновлением антивирусных баз	Еженедельно	
Контроль состава технических средств и средств защиты информации, применяемых в информационных системах персональных данных	Ежемесячно	
Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации	Еженедельно	
Контроль работоспособности, параметров настройки и правильности функционирования средств защиты информации	Ежемесячно	
Проверка журналов средств защиты информации для своевременного обнаружения фактов несанкционированного доступа к персональным данным	Еженедельно	
Контроль соблюдения правил эксплуатации криптосредств, хранения криптосредств, эксплуатационной документации к ним	Ежемесячно	
Контроль обеспечения резервного копирования, проверка работоспособности резервных копий	Ежемесячно	
Контроль правил генерации и смены паролей пользователей	Раз в три месяца	

Контроль реализации правил разграничения доступа, полномочий пользователей в информационных системах персональных данных согласно матрице доступа и исполненным заявкам	Раз в полгода	
Контроль работоспособности, параметров настройки и правильности функционирования, установленного (инсталлированного) в информационных системах персональных данных программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке в информационной системе персональных данных	Раз в три месяца	
Контроль заведения и удаления учетных записей пользователей	Прием/увольнение работника	Системный администратор
	Раз в три месяца	
Пересмотр организационно-распорядительной документации, регламентирующей порядок обработки персональных данных и требования по защите персональных данных, с учетом проводимых мероприятий по контролю	Ежегодно	Начальник отдела информационной безопасности и документооборота
	По факту изменения целей, технологии или иного значимого аспекта информационной безопасности	
Поддержание в актуальном состоянии организационно-распорядительных документов	Ежегодно	

Приложение 2 Лист периодичности внутренних проверок режима обработки и защиты персональных данных в автоматизированных информационных системах
(обязательное)

Мероприятие	Периодичность
Проверка соответствия состава и структуры программно-технических средств АИС документированному составу и структуре средств, представленному в техническом паспорте АИС	1 раз в 6 месяцев
Проверка выполнения требований по условиям расположения средств вычислительной техники в помещениях, в которых размещены элементы АИС	1 раз в 6 месяцев
Проверка организации допуска лиц в помещения, где размещены средства АИС, в т. ч. перечня лиц, имеющих право доступа в помещения АИС	1 раз в 6 месяцев
Проверка актуальности перечня лиц, допущенных к работе в АИС	1 раз в 6 месяцев
Проверка соответствия реального уровня полномочий по доступу к информации различных пользователей, установленному в матрице доступа	1 раз в 6 месяцев
Проверка организации учета средств защиты информации, используемых в АИС	1 раз в 6 месяцев
Проверка наличия документов, подтверждающих возможность применения технических и программных средств защиты информации (сертификатов соответствия и других документов)	1 раз в год
Проверка неизменности настроенных параметров средств защиты информации, используемых в АИС	1 раз в 6 месяцев
Контроль состава программного обеспечения	1 раз в 6 месяцев
Контроль правил заведения и удаления учетных записей пользователей	1 раз в 6 месяцев
Проверка соблюдения установленных правил организации парольной защиты	1 раз в 6 месяца
Контроль соблюдения установленных правил организации антивирусной защиты	1 раз в 6 месяца
Проверка работоспособности системы резервного копирования	1 раз в 6 месяцев
Проверка организации учета и условий хранения машинных носителей информации	1 раз в год
Проверка знаний персоналом базы нормативно-методических документов по защите информации	1 раз в год
Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения ФЗ-152 «О персональных данных»	1 раз в год
Проверка соответствия принимаемых мер необходимым мерам по обеспечению безопасности ПДн	1 раз в 6 месяцев
Организация анализа и пересмотра имеющихся угроз безопасности информации АИС, а также предсказание появления новых, еще неизвестных, угроз	Не реже 1 раз в год

Приложение 3 Форма протокола результатов проведения внутренней проверки

(обязательное)

П Р О Т О К О Л №_____
результатов проведения внутренней проверки
обеспечения безопасности информации

Настоящий Протокол составлен в том, что «___» _____ 20__ года Комиссией в составе:

Проверка осуществлялась в соответствии с требованиями: _____

_____

(название внутреннего локального акта)

_____

(должность, Ф.И.О. работника)

_____

(должность, Ф.И.О. работника)

была проведена плановая внутренняя проверка обеспечения безопасности информации.

Проверка осуществлялась в соответствии с требованиями: _____

_____

(название внутреннего локального акта)

В ходе проверки проверено:

_____

_____

_____

_____

_____

Выявленные нарушения:

_____

_____

_____

_____

Меры по устранению нарушений:

_____

_____

Срок устранения нарушений: _____

Проверку провели:

Члены комиссии:

_____ _____

(подпись) (Ф.И.О.)

_____ _____

(подпись) (Ф.И.О.)

_____ _____

(подпись) (Ф.И.О.)

_____ _____

(подпись) (Ф.И.О.)

«___» _____ 20__ года

Приложение 4 Форма акта выявления нарушений в сфере защиты персональных данных

(обязательное)

АКТ №_____
выявления нарушений в сфере защиты персональных данных

«_____» _____ 20_____

Настоящий акт составлен в том, что в

_____
(наименование структурного подразделения, где выявлено нарушение)

_____
(ФИО и должность лица, допустившего нарушение)

допущено нарушение установленных требований в сфере защиты персональных данных и иной конфиденциальной информации.

Содержание нарушения _____

Требования каких нормативных документов нарушены

_____

_____

Комиссия (или уполномоченное лицо), выявившая нарушения
Подписи:

_____ _____
(подпись) (Ф. И. О.)

_____ _____
(подпись) (Ф. И. О.)

С актом ознакомлены:
подпись лица, допустившего нарушение _____ _____
(подпись) (Ф. И. О.)

подпись начальника структурного подразделения, где допущено нарушение _____ _____
(подпись) (Ф. И. О.)

Приложение 5 Лист согласования Инструкции по организации контроля эффективности защиты информации в АИС

(обязательное)

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Дата	Подпись
Проректор по кампусному и корпоративному управлению	С.С. Аносов	12.04.2022	
И.о. проректора по международной деятельности	С.С. Быков	13.04.2022	
И.о директора департамента хозяйственной деятельности	Л.М. Чеботнягин	14.04.2022	
Проректор по научной работе	А.М. Кононов	13.04.2021	
Проректор по цифровой трансформации	А.Н. Копайгородский	25.01.2022	
Советник ректора	Е.Г. Можаева	12.04.2021	
Проректор по работе с госорганами и индустриальными партнерами	Е.Ю. Семёнов	04.02.22г.	
Проректор по учебной работе	В.В. Смирнов	17.02.2022	
Советник ректора по комплексной безопасности и международным связям	С.К. Филиппов	04.02.2022г.	
Начальник управления по работе с персоналом и обучающимися	Т.Ю. Гуруленко	13.04.2021	
Начальник управления планирования, бухгалтерского учета и аудита	Н.Б. Максимова	12.04.2021	
Начальник управления по дополнительному образованию и социальной работе	Б.Б. Пономарев	12.04.2021	
Начальник управления информатизации	В.В. Шмелев	19.01.22	
Руководитель юридической службы	О.Л. Пенизева	01.01.2022	
Заместитель начальника отдела мониторинга и качества образовательных услуг	О.С. Артемова	19.01.2022	

РАЗРАБОТАНО:

Начальник отдела информационной безопасности и документооборота	Л.В. Бархатова	19.01.2022	

Приложение 6 Лист регистрации изменений Инструкции по организации контроля эффективности защиты информации в АИС

(обязательное)

Порядковый номер изменения	**Основание (№ приказа, дата)**	**Дата введения изменения**	**Изменения внёс**	
			Фамилия, инициалы	**Подпись вносившего изменения, дата внесения**
1	2	3	4	5

Приложение 7 Лист ознакомления с Инструкцией по организации контроля эффективности защиты информации в АИС

(обязательное)

№	И.О. Фамилия	Должность	Дата	Подпись