КАМЧАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. ВИТУСА БЕРИНГА

Введено в действие приказом ФГБОУ ВО «КамГУ им. Витуса Беринга» № 39-ОД от 21.02.2024

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных, обрабатываемых федеральным государственным бюджетным образовательным учреждением высшего образования «Камчатский государственный университет имени Витуса Беринга» в информационных системах

ПОЛОЖЕНИЕ	Редакция 1	2024
Положение об обеспечении безопасности персональных данных, обрабатываемых федеральным государственным бюджетным образовательным учреждением высшего образования «Камчатский государственный университет имени Витуса Беринга» в информационных системах		

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер п/п	Основание для внесения изменений	Текст изменения	Дата внесения изменения

1. Общие положения

1.1. Положение об обеспечении безопасности персональных данных, обрабатываемых федеральным государственным бюджетным образовательным учреждением высшего образования «Камчатский государственный университет имени Витуса Беринга» в информационных системах (далее – Положение), разработано в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативными правовыми актами (методическими документами) федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.2. Настоящее Положение определяет состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн.

1.3. Положение обязательно для исполнения всеми работниками ФГБОУ ВО «КамГУ им. Витуса Беринга» (далее – Университет), непосредственно осуществляющими защиту ПДн, обрабатываемых в ИСПДн.

1.4. Настоящее положение включает в себя следующие правила и процедуры обработки персональных данных с использованием средств автоматизации:

1.4.1. Правила и процедуры идентификации и аутентификации субъектов доступа к объектам доступа (приложение 1).

1.4.2. Правила и процедуры управления доступом субъектов доступа к объектам доступа (приложение 2.

1.4.3. Правила и процедуры регистрации событий безопасности (приложение 3).

1.4.4. Правила и процедуры антивирусной защиты (приложение 4).

1.4.5. Правила и процедуры контроля (анализа) защищенности персональных данных (приложение 5).

1.4.6. Правила и процедуры защиты технических средств (приложение 6).

1.4.7. Правила и процедуры защиты информационной системы, ее средств, систем связи и передачи данных (приложение 7).

2. Термины и определения

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Основные технические средства и системы – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработ-

ки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3. Цели и задачи обеспечения безопасности персональных данных

3.1. Основной целью обеспечения безопасности ПДн при их обработке в ИСПДн является защита ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

3.2. Задачей, которую необходимо решить для достижения поставленной цели, является обеспечение безопасности ПДн при их обработке в ИСПДн с помощью системы защиты персональных данных (далее – СЗПДн), нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3.3. СЗПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в ИСПДн.

4. Основные принципы построения системы защиты информации

4.1. СЗПДн основывается на следующих принципах:

- системности;
- комплексности;
- непрерывности защиты;
- разумной достаточности;
- гибкости;
- простоты применения средств защиты информации (далее – СЗИ).

4.2. Принцип системности – предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн.

4.3. Принцип комплексности – предполагает, что СЗПДн должна включать совокупность объектов защиты, сил и средств, принимаемых мер, проводимых мероприятий и действий по обеспечению безопасности ПДн от возможных угроз всеми доступными законными средствами, методами и мероприятиями.

4.4. Принцип непрерывности защиты – это процесс обеспечения безопасности ПДн, осуществляемый руководством, ответственным за обеспечение безопасности ПДн в ИСПДн и работниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность СЗИ, сколько

процесс, который должен постоянно идти на всех уровнях внутри Учреждение, и каждый работник должен принимать участие в этом процессе.

4.5. Принцип разумной достаточности – предполагает соответствие уровня затрат на обеспечение безопасности ПДн ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.

4.6. Принцип гибкости – СЗПДн должна быть способна реагировать на изменения внешней среды и условий осуществления своей деятельности.

4.7. Принцип простоты применения СЗИ – механизмы защиты должны быть интуитивно понятны и просты в применении. Применение СЗИ не должно быть связано со знанием каких-либо языков или требовать дополнительных затрат на её применение, а также не должно требовать выполнения рутинных малопонятных операций.

5. Основные мероприятия по обеспечению безопасности персональных данных

5.1. Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, проводятся следующие мероприятия:

– определение ответственных лиц за обеспечение защиты ПДн;
– определение актуальных угроз безопасности ПДн;
– определение уровня защищенности ПДн;
– реализация правил разграничения доступа и введение ограничений на действия пользователей ИСПДн;
– ограничение доступа в помещения, где размещены основные технические средства и системы, позволяющие осуществлять обработку ПДн;
– учет и хранение съемных машинных носителей ПДн;
– организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ;
– организация парольной защиты;
– организация антивирусной защиты;
– организация обновления программного обеспечения и СЗИ;
– использование СЗИ;
– оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию СЗПДн;
– обнаружение фактов несанкционированного доступа к ПДн и принятие мер;
– контроль за принимаемыми мерами по обеспечению безопасности ПДн;
– планирование мероприятий по защите ПДн в ИСПДн;
– управление (администрирование) СЗПДн;
– управление конфигурацией ИСПДн и СЗПДн;
– реагирование на инциденты;
– информирование и обучение персонала ИСПДн.

5.2. Определение ответственных лиц за обеспечение безопасности ПДн

За вопросы обеспечения безопасности ПДн, обрабатываемых в ИСПДн, отвечают:

– Ответственный за организацию обработки ПДн – работник, отвечающий за организацию и состояние процесса обработки ПДн.

– Ответственный за обеспечение безопасности ПДн в ИСПДн – работник, отвечающий за правильность использования и нормальное функционирование установленной СЗПДн.

– Администратор ИСПДн – работник, отвечающий за правильность использования и бесперебойное, стабильное функционирование установленных систем обработки ПДн.

5.3. Определение актуальных угроз безопасности ПДн в ИСПДн

5.3.1. Актуальные угрозы безопасности ПДн, обрабатываемых в ИСПДн, определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей ИСПДн, возможных способов реализации угроз безопасности ПДн и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

5.3.2. Для определения угроз безопасности ПДн и разработки «Модели угроз безопасности персональных данных» применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. №1085.

5.4. Определение уровня защищенности ПДн

Уровень защищенности ПДн, обрабатываемых в ИСПДн, определяется в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и оформляется в виде «Акта об определения уровня защищенности персональных данных».

5.5. Реализация правил разграничения доступа и введение ограничений на действия пользователей ИСПДн

5.5.1. Реализация правил разграничения доступа, к ПДн, обрабатываемым в ИСПДн, осуществляется в соответствии с «Положением о разрешительной системе доступа в информационных системах персональных данных ФГБОУ ВО «КамГУ им. Витуса Беринга», утвержденным приказом ректора ФГБОУ ВО «КамГУ им. Витуса Беринга».

5.5.2. Основные технические средства и системы ИСПДн располагаются в помещениях, находящихся в пределах границы контролируемой зоны, определенной приказом ректора ФГБОУ ВО «КамГУ им. Витуса Беринга», с максимальным удалением от её границ.

5.5.3. Доступ в помещения, в которых ведется обработка ПДн, осуществляется в соответствии с «Правилами доступа работников в помещения, в которых ведется обработка персональных данных в ФГБОУ ВО «КамГУ им. Витуса Беринга», утвержденными приказом ректора ФГБОУ ВО «КамГУ им. Витуса Беринга».

5.6. Учет и хранение съемных машинных носителей ПДн

Работа со съемными машинными носителями ПДн в ИСПДн осуществляется в соответствии с «Порядком обращения со съемными машинными носителями персональных данных в Краткое название организации, утвержденным приказом ректора ФГБОУ ВО «КамГУ им. Витуса Беринга».

5.7. Организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ.

Организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ в ИСПДн осуществляется в соответствии с «Инструкцией по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных ФГБОУ ВО «КамГУ им. Витуса Беринга», утвержденной приказом ректора ФГБОУ ВО «КамГУ им. Витуса Беринга».

5.8. Организация парольной защиты

Организация парольной защиты в ИСПДн осуществляется в соответствии с «Инструкцией по парольной защите информации в ФГБОУ ВО «КамГУ им. Витуса Беринга», утвержденной приказом ректора ФГБОУ ВО «КамГУ им. Витуса Беринга».

5.9. Организация антивирусной защиты

Организация антивирусной защиты в ИСПДн осуществляется в соответствии с «Инструкцией по организации антивирусной защиты в ФГБОУ ВО «КамГУ им. Витуса Беринга», утвержденной приказом ректора ФГБОУ ВО «КамГУ им. Витуса Беринга».

5.10. Организация обновления программного обеспечения и СЗИ

Организация обновления программного обеспечения и СЗИ в ИСПДн осуществляется в соответствии с «Инструкцией ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных ФГБОУ ВО «КамГУ им. Витуса Беринга» и «Инструкцией администратора информационных систем персональных данных ФГБОУ ВО «КамГУ им. Витуса Беринга», утвержденные приказом ректора ФГБОУ ВО «КамГУ им. Витуса Беринга».

5.11. Применение СЗИ

5.11.1. Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, применяются СЗИ, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации, в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

5.11.2. Установка и настройка СЗИ в ИСПДн проводится в соответствии с эксплуатационной документацией на СЗПДн и документацией на СЗИ.

5.12. Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию СЗПДн

На этапах внедрения СЗПДн проводится оценка эффективности принимаемых мер по обеспечению безопасности ПДн, которая включает в себя:

- предварительные испытания СЗПДн;
- опытную эксплуатацию СЗПДн;
- анализ уязвимостей ИСПДн и принятие мер по их устранению;
- приемочные испытания СЗПДн.

5.13. Обнаружение фактов несанкционированного доступа к ПДн и принятие мер

5.13.1. Ответственному за обеспечение безопасности ПДн в ИСПДн или администратору ИСПДн должны сообщаться любые инциденты информационной безопасности, в которые входят:

- факты попыток и успешной реализации несанкционированного доступа в ИСПДн;
- факты попыток и успешной реализации несанкционированного доступа в помещения, в которых ведется обработка ПДн;
- факты сбоя или некорректной работы систем обработки ПДн;
- факты сбоя или некорректной работы СЗИ;
- факты разглашения ПДн, обрабатываемых в ИСПДн;
- факты разглашения информации о методах и способах защиты и обработки ПДн в ИСПДн.

5.13.2. Разбор инцидентов информационной безопасности проводится в соответствии с «Регламентом реагирования на инциденты информационной безопасности в информационных системах персональных данных ФГБОУ ВО «КамГУ им. Витуса Беринга», утвержденным приказом ректора ФГБОУ ВО «КамГУ им. Витуса Беринга».

5.14. Контроль за принимаемыми мерами по обеспечению безопасности ПДн

Контроль за принимаемыми мерами по обеспечению безопасности ПДн осуществляется в соответствии с «Регламентом проведения внутреннего контроля соответствия обработки персональных данных в ФГБОУ ВО «КамГУ им. Витуса Беринга», утвержденным приказом ректора ФГБОУ ВО «КамГУ им. Витуса Беринга».

6. Ответственность

6.1. Все работники, допущенные в установленном порядке к работе с ПДн, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством Российской Федерации за необеспечение сохранности и несоблюдение правил работы с ПДн.

6.2. Ответственность за доведение требований настоящего Положения до работников ФГБОУ ВО «КамГУ им. Витуса Беринга» и обеспечение мероприятий по их реализации несет ответственный за обеспечение безопасности ПДн в ИСПДн.

Приложение 1

Правила и процедуры идентификации и аутентификации субъектов доступа к объектам доступа

1. Правила и процедуры идентификации и аутентификации включают в себя регламентацию следующих правил и процедур:

1.1. Правила и процедуры идентификации и аутентификации пользователей, являющихся работниками Университета.

1.2. Правила и процедуры управления идентификаторами.

1.3. Правила и процедуры управления средствами аутентификации (аутентификационной информацией).

1.4. Правила и процедуры защиты обратной связи при вводе аутентификационной информации.

1.5. Правила и процедуры идентификации и аутентификации внешних пользователей.

2. Правила и процедуры идентификации и аутентификации пользователей, являющихся работниками Университета

2.1. Идентификация и аутентификация пользователей, являющихся работниками Университета (далее – внутренние пользователи), должна производиться техническими средствами и системами, содержащими службы каталогов (Microsoft Active Directory, OpenLDAP, Samba и др.).

2.1.1. К внутренним пользователям относятся должностные лица Университета, выполняющие свои должностные обязанности с использованием информации, информационных технологий, информационной системы и технических средств информационной системы в соответствии с должностными регламентами, и которым в ИСПДн также присвоены учетные записи.

2.1.2. Идентификация внутренних пользователей должна осуществляться по уникальным учетным записям, которые однозначно идентифицируют пользователя. Запрещается применять учетные неидентифицируемые учетные записи, например, "user", "пользователь", "administrator" и т.д.

2.1.3. В качестве идентификаторов внутренних пользователей должен использоваться логин службы каталогов.

2.1.4. Допускается использование иных идентификаторов внутренних пользователей, таких как: уникальное устройство (iButton, eToken, RuToken, iKey, смарт-карты и др.); электронная подпись.

2.1.5. Для каждого идентификатора должна быть определена следующая информация о пользователе: фамилия, имя, отчество пользователя, должность.

2.1.6. Учет идентификаторов, выданных внутренним пользователям, производится:

- средствами службы каталогов;
- в журнале учета идентификаторов;
- в журнале учета средств криптографической защиты информации удостоверяющего центра.

2.1.7. Типовые формы учета идентификаторов разрабатываются администратором информационной безопасности (далее — Администратор ИБ).

2.1.8. Для аутентификации внутренних пользователей могут использоваться следующие факторы аутентификации:

– пароль, пин-код;
– уникальное устройство аутентификации: iButton, eToken, RuToken, iKey, смарт-карты и др.;
– биометрия.

2.1.9. Допускается в качестве усиления процедур аутентификации использовать комбинации факторов аутентификации информационных систем.

3. Правила и процедуры управления идентификаторами

3.1. Администратор ИБ является лицом, ответственным за создание, присвоение и уничтожение идентификаторов пользователей.

3.2. Запрещается повторно использовать идентификатор пользователя в течение не менее 1 года.

3.3. Администратор ИБ обязан блокировать или инициировать блокировку идентификаторов пользователей через период времени неиспользования не более 90 дней.

4. Правила и процедуры управления средствами аутентификации (аутентификационной информацией).

4.1. Администратор ИБ является лицом, ответственным за хранение, выдачу, инициализацию, блокирование средств аутентификации.

4.2. На всех средствах вычислительной техники Администратор ИБ должен осуществлять изменение аутентификационной информации (средств аутентификации), заданной их производителями.

4.3. Администратор ИБ устанавливает и регистрирует по средством СЗИ следующие характеристики паролей: длина пароля; алфавит пароля (при наличии соответствующих механизмов); максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки программно-технического средства или учетной записи пользователя; время блокировки программно-технического средства или учетной записи пользователя после превышения количества неуспешных попыток аутентификации (ввода неправильного пароля); максимальное время действия пароля; минимальное время действия пароля.

4.4. В случае компрометации или подозрения компрометации паролей, пользователь ИСПДн обязан незамедлительно обратиться к Администратору ИБ.

4.5. Администратор ИБ после сообщения компрометации обязан осуществить незамедлительное блокирование скомпрометированных средств аутентификации. При необходимости, информация о компрометации сообщается руководителю Университета или его заместителю.

4.6. Доступ к администрированию технических средств и систем, содержащим службы каталогов, должен быть предоставлен только Администратору ИБ.

5. Правила и процедуры защиты обратной связи при вводе аутентификационной информации.

5.1. Администратор ИБ обеспечивает исключение отображения для пользователя ИСПДн действительного значения аутентификационной информации (пароля) путем:
– использования встроенных средств защиты обратной связи (вводимые символы отображаются условными знаками "*", "|");
– доработки прикладного программного обеспечения с целью установления средства защиты обратной связи (вводимые символы отображаются условными знаками "*", "|").

5.2. Пользователю ИСПДн запрещается ввод аутентификационной информации в случае, если существует возможность наблюдения за вводом со стороны посетителей или посторонних лиц.

Приложение 2

Правила и процедуры управления доступом субъектов доступа к объектам доступа

1. Правила и процедуры управления доступом субъектов доступа к объектам доступа включают в себя регламентацию следующих правил и процедур:

1.1. Правила и процедуры управления учетными записями пользователей.

1.2. Правила разграничения доступа.

1.3. Правила и процедуры управления информационными потоками между устройствами и сегментами информационной системы.

1.4. Правила и процедуры разделения полномочий пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.

1.5. Правила и процедуры назначения минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.

1.6. Правила и процедуры ограничения неуспешных попыток входа.

1.7. Правила и процедуры разрешения (запрета) действий пользователей, разрешенных до идентификации и аутентификации.

1.8. Правила и процедуры применения удаленного доступа.

1.9. Правила и процедуры применения технологий беспроводного доступа.

1.10. Правила и процедуры применения мобильных технических средств.

1.11. Правила и процедуры управления взаимодействием с внешними информационными системами.

2. Правила и процедуры управления учетными записями пользователей.

2.1. Пользователями ИСПДн могут являться только штатные сотрудники Университета.

2.2. Пользователи ИСПДн должны иметь возможность работать только с теми средствами и ресурсами ИСПДн, которые необходимы им для выполнения установленных функциональных обязанностей.

2.3. По умолчанию, все создаваемые администратором информационной безопасности (далее – Администратором ИБ) учетные записи, являются учетными записями внутренних пользователей.

2.4. При создании Администратором ИБ учетных записей, не принадлежащих сотрудникам Университета, в описании учетной записи должна быть добавлена информация о типе создаваемой учетной записи (внешний пользователь; системная, приложения; гостевая (анонимная), временная и (или) иной тип записи).

2.5. Для разграничения прав доступа к ресурсам ИСПДн могут использоваться следующие методы разграничения доступа:

- дискреционный (управление доступом для индивидуального субъекта доступа);
- ролевой (управление доступом по группам субъектов доступа);
- мандатный (сопоставление классификационных меток каждого субъекта доступа и каждого объекта доступа).

2.6. Методы разграничения доступа в ИСПДн определяются на этапе проектирования ИСПДн или в процессе функционирования ИСПДн Администратором ИБ и фиксируются в техническом паспорте ИСПДн.

2.7. Управление учетными записями в ИСПДн:

создание новой учетной записи в ИСПДн осуществляется Администратором ИБ;

– учетная запись внутреннему пользователю создается на основании служебной записки на имя ректора Университета либо его заместителя;
– присвоение учетной записи производится в технических средствах системами, содержащими службы каталогов (Microsoft Active Directory, OpenLDAP, Samba и др.) с внесением данных, указанных в п. 2.4 Правил и процедур идентификации и аутентификации субъектов доступа к объектам доступа;
– выдача учетных данных внутренним пользователям производится на бумажном носителе лично в руки субъекту доступа или его непосредственному руководителю.

2.8. Не реже 1 раза в 180 дней Администратор ИБ проводит пересмотр (актуализацию) учетных записей и прав доступа. В ИСПДн не должно быть неиспользуемых учетных записей или учетных записей с истекшим сроком действия, регламентированным правилами и процедурами идентификации и аутентификации субъектов доступа и объектов доступа.

2.9. Временные учетные записи:
– временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для произведения настройки, тестирования информационной системы, для организации гостевого доступа;
– после выполнения задач, временная учетная запись должна быть заблокирована или удалена Администратором ИБ;
– при создании временных учетных записей срок их действия контролируется вручную Администратором ИБ или автоматически (средствами службы каталогов).

3. Правила разграничения доступа.

3.1. Для всех технических средств и систем ИСПДн, содержащих службы каталогов, Администратором ИБ должны быть разработаны разрешительные системы доступа субъектов доступа к объектам доступа (матрица доступа).

3.2. В матрице доступа должны быть определены права доступа (операции воздействия) субъектов доступа на объекты доступа (полный доступ, чтение, запись, удаление, выполнение и др.), реализуемые в ИСПДн.

3.3. Администратором ИБ должно быть обеспечено назначение прав и привилегий пользователям, минимально необходимых для выполнения ими своих должностных обязанностей.

4. Правила и процедуры управления информационными потоками между устройствами и сегментами информационной системы.

4.1. Администратор ИБ обеспечивает для ИСПДн управление информационными потоками:
– методом фильтрации информационных потоков по принципу «запрещено все, кроме разрешенного сетевого трафика»;
– установка маршрутов информационных потоков по принципу «запрещены все, кроме разрешенных маршрутов»;
– администратором ИБ, в случае необходимости, производится изменение маршрута передачи информации, о чем должны быть внесены соответствующие изменения в технический паспорт системы;
– при транзитной передаче информации Администратор ИБ принимает решение о необходимости записи передаваемых данных во временное хранилище информации для анализа и принятия решения.

5. Правила и процедуры разделения полномочий пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.

5.1. Администратором ИБ разрабатывается разрешительная система доступа к ИСПДн, регламентирующая разделение полномочий пользователей ИСПДн в соответствии с их должностными функциями.

6. Правила и процедуры назначения минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.

6.1. Администратор ИБ устанавливает минимальные необходимые права и привилегии пользователям, необходимые для выполнения их функциональных обязанностей.

6.2. Права на доступ пользователей к ресурсам ИСПДн устанавливаются в разрешительной системе доступа.

7. Правила и процедуры ограничения неуспешных попыток входа.

7.1. Параметры ограничения неуспешных попыток входа определяются Администратором ИБ.

7.2. Необходимые параметры ограничений:

– длина пароля не менее 6 символов;
– алфавит пароля не менее 60 символов;
– пороговое значение блокировки – не менее 3 ошибок входа в систему;
– продолжительность блокировки учетной записи – не менее 5 минут;
– смена пароля не более чем через 120 дней.

8. Правила и процедуры разрешения (запрета) действий пользователей, разрешенных до идентификации и аутентификации.

8.1. При необходимости Администратор ИБ устанавливает перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет действий пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации. Данные функциональные возможности реализуются путем разрешения (запрета) действий пользователей, разрешенных до идентификации и аутентификации (гостевые учетные записи) при помощи локальной (групповой доменной) политики безопасности.

8.2. Перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации: локальный вход на АРМ под гостевой учетной записью.

9. Правила и процедуры применения удаленного доступа.

9.1. Под удаленным доступом понимается процесс получения доступа (через внешнюю сеть) к объектам доступа ИСПДн из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с информационной системой, к которой он получает доступ.

9.2. Защита удаленного доступа к ресурсам ИСПДн осуществляется с использованием защищенных каналов связи (VPN, шифрование и т.д.).

9.3. Виды удаленного доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) для ИСПДн устанавливаются на этапе проектирования ИСПДн, модифицируются в процессе ее использования и регламентируются Администратором ИБ в техническом паспорте ИСПДн.

9.4. Для ИСПДн должно использоваться ограниченное (минимально необходимое) количество точек подключения при организации удаленного доступа.

9.5. Для ИСПДн запрещен удаленный доступ от имени привилегированных учетных записей (администраторов) для администрирования ИСПДн и ее систем защиты информации.

9.6. Администратор ИБ осуществляет контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа ИСПДн.

10. Правила и процедуры применения технологий беспроводного доступа.

10.1. При применении технологии беспроводного доступа в сети общего пользования Администратором ИБ обеспечивается:

- сегментирование (межсетевое экранирование) компьютера, при этом правила фильтрации межсетевого экрана должны обеспечивать запрет любого входящего трафика, кроме разрешенного;
- шифрование передаваемых данных при передаче информации.

11. Правила и процедуры применения мобильных технических средств.

11.1.В ИСПДн запрещено использование мобильных технических средств (кроме стационарных в соответствии с установленными правилами и процедурами защиты информационной системы, ее средств, систем связи и передачи данных).

12. Правила и процедуры управления взаимодействием с внешними ИС.

12.1. В ИСПДн осуществляется взаимодействие со следующими внешними информационными системами:

- Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» обеспечивает идентификацию и аутентификацию пользователей ИСПДн;
- Государственная информационная система «Современная цифровая образовательная среда».

12.2. Разрешение обработки, хранения и передачи защищаемой информации с использованием внешних информационных систем в ИСПДн возможно только при выполнении следующих условий:

- при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;
- при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

12.3. Для ИСПДн устанавливается возможность использования системных учетных записей, что должно быть отражено в техническом паспорте ИСПДн. Решение по использованию в ИСПДн системных учетных записей принимается Администратором ИБ.

Приложение 3

Правила и процедуры регистрации событий безопасности

1. Правила и процедуры регистрации событий безопасности включают в себя регламентацию следующих правил и процедур:

1.1. Правила и процедуры определения событий безопасности.

1.2. Правила и процедуры определения состава и содержания информации о событиях безопасности.

1.3. Правила и процедуры сбора, записи и хранения информации о событиях безопасности.

1.4. Правила и процедуры защиты информации о событиях безопасности.

2. Правила и процедуры определения событий безопасности.

2.1. Для ИСПДн администратор информационной безопасности (далее — Администратор ИБ) определяет перечень событий безопасности, подлежащие регистрации. Перечень определяется на этапе проектирования ИСПДн, модифицируются в процессе ее использования.

2.2. События безопасности, подлежащие регистрации, должны определяться Администратором ИБ с учетом способов реализации угроз безопасности для ИСПДн.

2.3. Для каждого типа событий Администратор ИБ определяет минимальный срок хранения журналов событий, регламентирует его в перечне регистрируемых событий.

2.4. События безопасности, а также сроки хранения должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИСПДн.

3. Правила и процедуры определения состава и содержания информации о событиях безопасности.

3.1. Для каждого регистрируемого типа событий безопасности Администратор ИБ определяет состав и содержание информации о событиях безопасности.

3.2. Состав и содержание информации о событиях безопасности должны обеспечивать возможность идентификации:

- типа события безопасности;
- даты и времени события безопасности;
- идентификационной информации источника события безопасности;
- результат события безопасности;
- субъект доступа.

4. Правила и процедуры сбора, записи и хранения информации о событиях безопасности.

4.1. Администратор ИБ обеспечивает регистрацию событий безопасности, а также устанавливает состав и содержание регистрируемой информации с использованием средств защиты информации, установленных в ИСПДн.

4.2. Объем памяти для хранения информации о событиях безопасности рассчитывается Администратором ИБ с учетом типов событий безопасности, их состава, содержания, прогнозируемой частоты возникновения, а также срока их хранения.

5. Методы защиты информации о событиях безопасности.

5.1. В ИСПДн Администратором ИБ используются следующие методы защиты информации о событиях безопасности:

- логическое ограничение доступа к местам хранения журналов событий;

– управление журналами событий. Доступ к управлению журналами должен быть разрешен только для привилегированных пользователей ИСПДн.

9.2. Контроль реализации методов защиты осуществляется Администратором ИБ не реже 1 раза в год.

Приложение 4

Правила и процедуры антивирусной защиты

1. Правила и процедуры антивирусной защиты включают в себя регламентацию следующих правил и процедур:

1.1. Правила и процедуры антивирусной защиты.

1.2. Правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов).

2. Правила и процедуры антивирусной защиты.

2.1. Средства антивирусной защиты (далее – АВЗ) применяются:

- на автоматизированных рабочих местах (далее – АРМ);
- на серверах;
- в периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), где существует техническая возможность;
- мобильных технических средствах;
- иных точках доступа в ИСПДн.

2.2. В ИСПДн должны применяться только сертифицированные по требованию безопасности средства АВЗ.

2.3. Установка, конфигурирование и управление средствами АВЗ осуществляется Администратором ИБ.

2.4. Параметры настройки средств АВЗ определяются Администратором ИБ в соответствии с технической документацией.

2.5. На АРМ проводятся следующие виды антивирусных проверок:

- быстрая проверка – при загрузке операционной системы;
- полная проверка – не реже 1 раза в неделю;
- подключение съемных носителей информации – принудительно при каждом подключении.

2.6. На серверах проводятся следующие виды антивирусных проверок:

- быстрая проверка – при загрузке операционной системы;
- полная проверка – не реже 1 раза в неделю;
- подключение съемных носителей информации – принудительно при каждом подключении.

2.7. В периметральных средствах защиты информации проводится проверка в режиме реального времени.

2.8. В мобильных технических средствах:

- быстрая проверка – при загрузке операционной системы;
- полная проверка – не реже 1 раза в неделю;
- проверка устанавливаемого программного обеспечения – принудительно при каждой установке.

2.9. Доступ к консоли управления антивирусным средством ограничивается паролем с учетом требований парольной защиты в ИСПДн.

2.10. Пользователям запрещается отключать средства АВЗ и самостоятельно вносить изменения в их настройки.

2.11. Администратор ИБ производит установку парольного доступа к настройкам средств АВЗ.

2.12. При подключении внешних и съемных носителей информации в ИСПДн должна проводиться автоматическая быстрая проверка на наличие вирусных программ.

2.13. Должна проводиться автоматическая проверка объектов (файлов) при загрузке, открытии или исполнении таких файлов.

2.14. Управление средствами АВЗ, при наличии технической возможности, должно осуществляться централизованно.

2.15. В случае обнаружения вредоносных программ пользователи информационной системы обязаны:

- приостановить работу на своем компьютере;
- немедленно сообщить о факте заражения Администратору ИБ;
- возобновить работу только после удаления вирусной программы и нейтрализации последствий вирусного заражения.

2.16. В случае обнаружения вредоносных программ Администратор ИБ обязан:

- незамедлительно принять меры по удалению вирусной программы (лечению) и нейтрализации последствий вирусного заражения;
- при невозможности удаления (лечения) принять меры по нейтрализации возможности деструктивного воздействия со стороны вирусной программы.

2.17. Администратор ИБ, при необходимости, инициирует проведения служебного расследования по факту вирусного заражения.

3. Правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов).

3.1. Обновление сигнатур осуществляется в автоматическом режиме по заданному расписанию. Источником обновлений могут являться сервера обновлений производителей средств АВЗ.

3.2.Минимальная периодичность проверки и получения обновлений – 1 раз в сутки.

3.3. Запрещается устанавливать обновление ядра АВЗ.

4. Пользователь несет персональную ответственность за осуществление регламента использования на АРМ ИСПДн антивирусных средств.

Приложение 5

Правила и процедуры контроля (анализа) защищенности персональных данных

1. Правила и процедуры анализа защищенности информации включают в себя регламентацию следующих правил и процедур:

1.1. Правила и процедуры контроля установки обновлений программного обеспечения.

2. Правила и процедуры контроля установки обновлений программного обеспечения.

2.1. На всех элементах ИСПДн должен быть обеспечен запрет установки обновлений средств защиты информации (далее — СрЗИ) от имени непривилегированных пользователей.

2.2. Сертифицированные по требованиям безопасности информации СрЗИ должны обновляться с доверенных серверов сертифицированной поддержки продуктов.

2.3. Запрещается устанавливать настройки обновлений СрЗИ с общедоступных недоверенных источников обновлений.

2.4. Доверенным источником обновлений считается:

- источник обновлений, который указан в паспорте-формуляре СрЗИ;
- источник обновлений, который установлен по умолчанию при установке СрЗИ с сертифицированного дистрибутива продукта.

2.5. Установка обновлений операционных систем ИСПДн должна проводиться в автоматическом режиме с доверенных серверов сертифицированной поддержки продуктов операционных систем или установленного в локальной вычислительной сети Университета сервера обновлений (WSUS).

2.6. Установка обновлений прикладного и системного программного обеспечения проводиться Администратором ИБ.

2.7. Контроль установки обновлений осуществляет Администратор ИБ не реже одного раза в квартал.

2.8. Пользователь несет персональную ответственность за нарушение Правил и процедур анализа защищенности информации.

Приложение 6

Правила и процедуры защиты технических средств

1. Правила и процедуры защиты технических средств включают в себя регламентацию следующих правил и процедур:

1.1. Правила и процедуры организации контролируемой зоны.

1.2. Правила и процедуры контроля и управления физическим доступом к техническим средствам.

1.3. Правила и процедуры размещения устройств вывода (отображения) информации.

2. Правила и процедуры организации контролируемой зоны.

2.1. Контролируемая зона – это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

2.2. Контролируемая зона для технических средств ИСПДн определяется администратором информационной безопасности (далее — Администратор ИБ) и утверждается приказом ректора университета.

2.3. Для ИСПДн может быть организовано несколько контролируемых зон.

3. Правила и процедуры контроля и управления физическим доступом к техническим средствам.

3.1. В контролируемой зоне должен обеспечиваться контроль и управление физическим доступом к техническим средствам (далее — ТС).

3.2. Для обеспечения п. 3.1 применяются следующие технические средства:

- двери, расположенные по периметру контролируемой зоны, должны быть оборудованы механическим замком;
- окна, расположенные по периметру контролируемой зоны, должны быть оснащены системами открывания с внутренней стороны; дополнительно могут применяться системы контроля и управления доступом, металлические решетки на окнах, охранные датчики (движения, открытия, разбития стекол и т.д.), видеонаблюдение.

3.3. Для обеспечения п. 3.1 применяются следующие организационные меры:

- администратором ИБ составляются список лиц, допущенных к ТС, средствам защиты информации, средствам обеспечения функционирования, а также в помещения, в которых они установлены;
- всем лицам запрещается оставлять помещение незапертым в моменты отсутствия в нем лиц, допущенных в контролируемую зону;
- администратором ИБ осуществляется учет физического доступа сторонних лиц, не являющихся сотрудниками Университета и сотрудниками охранного предприятия Университета, к ТС, средствам защиты информации, средствам обеспечения функционирования, а также в помещения, в которых они установлены.

4. Правила и процедуры размещения устройств вывода (отображения) информации.

4.1. В качестве устройств вывода (отображения) информации в ИСПДн рассматриваются экраны мониторов автоматизированных рабочих мест пользователей.

4.2. Устройства вывода (отображения) информации должны располагаться таким образом, чтобы была исключена или сведена к минимуму возможность просмотра информации посторонними лицами.

4.3. Потенциальные направления визуального съема информации определяются Администратором ИБ.

4.4. Администратор ИБ контролирует расположение устройств вывода (отображения) информации и их изменение расположения пользователями.

Приложение 7

Правила и процедуры защиты информационной системы, ее средств, систем связи и передачи данных

1. Правила и процедуры информационной системы, ее средств, систем связи и передачи данных включают в себя регламентацию следующих правил и процедур:

1.1. Правила и процедуры обеспечения защиты информации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны.

2. Правила и процедуры обеспечения защиты информации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны.

2.1. Запрещается передача защищаемой информации по открытым каналам связи без применения сертифицированных по требованиям безопасности средств криптографической защиты информации.

РАЗРАБОТЧИК:
Первый проректор _____ О.А. Сулица
«___» _____ 2024 г.

СОГЛАСОВАНО:
Ведущий юрисконсульт _____ Э.О. Задорожняя
«___» _____ 2024 г.

НОРМОКОНТРОЛЬ:
И.о. начальника отдела оценки и
контроля качества деятельности
университета _____ И.А. Кашутина
«___» _____ 2024 г.

ЛИСТ ОЗНАКОМЛЕНИЯ

Должность	Ф.И.О.	Подпись	Дата