**РАЗРАБОТКА И АКТУАЛИЗАЦИЯ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ: ОПЫТ ВУЗа**

*Аннотация: Статья посвящена комплексному подходу к созданию и обновлению организационно-технической документации в сфере информационной безопасности (ИБ) на примере ВУЗа. В материале рассматриваются ключевые документы, такие как инструкции по работе с персональными данными, политики обработки данных, должностные инструкции для сотрудников отдела ИБ, а также технические регламенты и положения о лабораториях. Особое внимание уделяется актуализации существующих документов, таких как Общая политика ИБ, и внедрению новых требований, включая уведомления о сборе метаданных на сайте и инструкции по усовершенствованию веб-ресурсов.*

*Ключевые слова: организационно-техническая документация, информационная безопасность, образовательные учреждения.*

В современных условиях защита информации (ЗИ), представляющая собой комплекс мер различного характера, необходима для защиты конфиденциальной информации и информационного пространства от несанкционированного вмешательства, хищения и изменения информации со стороны третьих лиц.

Организация деятельности по ЗИ включает комплекс мер, направленных на обеспечение безопасности данных и информационных систем.

На первом этапе разрабатывается и утверждается политика ЗИ, которая определяет основные принципы, цели и задачи в этой области. Важным шагом является назначение лиц, ответственных за защиту информации, что позволяет четко распределить обязанности и обеспечить контроль за выполнением требований. Для реализации защитных мер применяются специализированные программные и программно-аппаратные средства, предназначенные для предотвращения угроз и минимизации рисков. Следующим этапом становится выделение необходимых организационных, технических и иных ресурсов, обеспечивающих эффективное функционирование системы ЗИ. Параллельно разрабатываются внутренние стандарты и регламенты, которые регламентируют процессы обработки, хранения и передачи информации.

По причине того, что в стандартах описываются требования по реализации мер ЗИ, а в регламентах – прядок их реализации, то для эффективной организации ЗИ важно, чтобы стандарты и регламенты были максимально приближены к исполнителям и понятны для их применения.

Кроме того, при разработке документации следует учитывать актуальные угрозы, типичные для образовательной среды, включая социальную инженерию, фишинг и несанкционированный доступ к системам дистанционного обучения. Разработка типовых шаблонов и чек-листов для структурных подразделений ВУЗа позволяет унифицировать подходы к защите информации и снизить вероятность ошибок. Также рекомендуется проводить регулярный пересмотр документов и проверку их применимости на практике с участием представителей ИБ, ИТ и юридической службы.

Рисунок 1 - Этапы разработки и сопровождения документации по ЗИ

К внутренним стандартам организации относятся нормативные требования, правила и критерии, которые устанавливают единые подходы к выполнению задач, обеспечению качества и безопасности процессов. Эти стандарты определяют, что должно быть сделано, и задают четкие ориентиры для сотрудников. В то же время регламенты описывают порядок, последовательность и методику выполнения этих требований, то есть как именно должны выполняться процессы. Регламенты детализируют шаги, сроки, ответственных лиц и взаимодействие между подразделениями, обеспечивая согласованность и эффективность работы. Примеры внутренних стандартов и регламентов представлены в табл. 1.

Таблица 1 – Примеры внутренних стандартов и регламентов

|  |  |
| --- | --- |
| **Внутренние стандарты** | Требования к обновлению ПО |
| Требования к созданию и использованию учетных записей (парольная политика, многофакторная аутентификация). |
| Перечень разрешенного и запрещенного ПО. |
| **Внутренние регламенты** | Порядок повышения уровня знаний и информированности пользователей по вопросам ЗИ |
| Регламент управления учетными записями |
| Порядок тестирования знаний по вопросам ИБ |
| Регламенты передачи данных |

ИБ является одной из ключевых задач для образовательных учреждений, особенно в условиях цифровой трансформации. Для её обеспечения необходимо учитывать следующие риски:

* утечка данных в результате действий сотрудников (человеческий фактор или умышленное преступление);
* несанкционированный доступ к информационным системам;
* несвоевременное обновление ПО и антивирусной защиты;
* нарушение требований законодательства;
* отсутствие инструктажа и обучения персонала ИБ.

В качестве дополнительной меры обеспечения безопасности информации предлагается реализовывать ежегодный аудит сотрудников ответственных за ИБ образовательного учреждения, повышать их квалификацию, оценку соответствия требованиям ИБ регулирующих документов и т.д, а также использовать DLP и SIEM системы, современные технологии, такие как Kryptos TLS Server [1], которые позволят обеспечить безопасность передачи данных, своевременный анализ и реагирование на инциденты.

ВУЗы ежегодно обрабатывают огромные массивы конфиденциальной информации, включая персональные данные студентов, сотрудников и научные разработки. Особенно остро вопрос ЗИ встаёт во время приёмной кампании, когда тысячи абитуриентов передают в вуз свои личные данные: паспортные сведения, результаты ЕГЭ, контактную информацию и другие данные. К сожалению, случаи утечки персональных данных в образовательных учреждениях не являются редкостью. Только за последние несколько лет были зафиксированы многочисленные инциденты, причём в абсолютно различных сферах:

Рисунок 2 – Статистика утечки ПДн из различных отраслей

Так, к примеру, 8 марта 2023 года хакеры выложили в открытый доступ два архива с данными из информационной системы Высшей школы экономики, включая сканы паспортов и персональные данные выпускников и сотрудников, списки сотрудников, имеющих отсрочку от мобилизации, досье абитуриентов магистратуры, логины и пароли для доступа к системе электронного документооборота и другим внутренним сервисам. В результате суд оштрафовал Высшую школу экономики на 60 тыс. рублей за утечку персональных данных сотрудников и студентов в соответствии с нарушением законодательства в области персональных данных по ч. 1 ст. 13.11 КоАП РФ.

А 13 декабря 2022 года в открытый доступ попали данные пользователей образовательного портала «Московская Электронная Школа». По информации экспертов сервиса поиска утечек и мониторинга даркнета DLBI, в опубликованном файле находятся 17056658 строк, содержащих данные зарегистрированных пользователей МЭШ (московских учителей, школьников и их родителей), включая:

* ФИО;
* номера телефонов (среди которых 3,6 миллионов уникальных номеров);
* адреса электронной почты (среди которых 5,5 миллионов уникальных адресов);
* даты рождения;
* СНИЛС;
* логин в системе.

На год позже, 17 января 2023 года компания «1С» столкнулась с утечкой данных зарегистрированных пользователей образовательного сервиса «1С:Урок». В открытый доступ был выложен файл с таблицей зарегистрированных пользователей из базы данных предположительного портала «1С:Урок», в котором содержатся почти 190 тысяч строк персональных данных, а именно:

* ФИО;
* номера телефонов (среди которых 7,5 тысяч уникальных номеров);
* адреса электронной почты (среди которых 185 тысяч уникальных адресов и т.д.

Утечки подобного рода относятся к нарушениям порядка обработки и хранения персональных данных, ответственность за данные нарушения установлена статьёй 13.11 КоАП РФ. Также, в случае утечки ПДн оператор обязан в течение 24 часов с момента выявления такого инцидента подать уведомление об их утечке в Роскомнадзор, в течение 72 часов с момента выявления инцидента о результатах его внутреннего расследования, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента.

Обеспечение безопасной обработки и хранения ПДн – одна из основных задач университета. На сегодняшний день ведётся активная работа по совершенствованию организационно-технических мер ЗИ: внедряются современные системы шифрования, строго регламентируется доступ к данным, проводится обучение сотрудников, работающих с персональными данными.

Соблюдение требований законодательства (в частности, ФЗ-152 «О персональных данных» [2]) и применение передовых технологий позволяют минимизировать риски утечек и обеспечить абитуриентам и студентам уверенность в сохранности их информации.

Игнорирование и несоблюдение требований, установленных федеральными законами Российской Федерации (РФ), влечёт за собой привлечение к ответственности в соответствии с КоАП РФ Статья 13.11 «Нарушение законодательства РФ в области персональных данных», ФЗ-152 «О персональных данных» от 27.07.2006 [2] и другими нормативно-правовыми актами РФ.

Также, с 30 мая 2025 года вступят в силу новые требования к операторам персональных данных (Федеральный закон от 30.11.2024 №420-ФЗ). Теперь за нарушение правил обработки персональных данных общей категории можно получить штраф до 500 млн руб., специальной категории — наказание в форме лишения свободы на срок до 5 лет.



Рисунок 3 – Штрафные санкции за нарушение требований законодательства для различных категорий лиц

Ниже, на рисунке 4, приведена ответственность за нарушение закона в сфере обработки и хранения ПДн в соответствии с положениями КоАП, трудового кодекса (ТК) и уголовного кодекса (УК) РФ.



Рисунок 4 – Ответственность за нарушение закона в сфере обработки и хранения ПДн

В случае наличия у ВУЗа филиалов в других городах необходимо учитывать особенности передачи конфиденциальной информации по телекоммуникационным сетям, такие как:

* уязвимость к несанкционированному доступу по причине открытости телекоммуникационных сетей для пользователей, что может привести к получению конфиденциальных данных или нарушению работы сети из-за атак типа «отказ в обслуживании»;
* использование разных протоколов связи с различным уровнем безопасности;
* применение правильного оборудования, которое предусматривает реализацию мер ЗИ, и технических средств, обеспечивающих защиту от несанкционированного доступа;
* подбор персонала, допускаемого к взаимодействию с конфиденциальными данными с целью уменьшить шансы на компрометацию персональных данных.

С точки зрения организационно-правовой ЗИ требуется разработать Регламент передачи данных, содержащий:

* условия передачи, при которых возможна передача данных (например, наличие согласия субъекта ПДн, служебная необходимость);
* способы передачи (электронная почта с шифрованием, защищенные каналы связи, VPN, специализированные системы обмена данными);
* форматы данных с указаниями допустимых форматов передачи (например, зашифрованные файлы, электронные подписи);
* процедура инициирования передачи, содержащий процесс инициирования и подтверждения передачи данных (например, заявка от одного филиала, утверждение ответственным лицом).

В области финансов, в частности выплаты стипендий студентам, происходит следующий порядок передачи данных:

1. Вуз формирует реестр (список) студентов с указанием всех необходимых данных:

* ПДн студентов — ФИО, дата рождения, ИНН, СНИЛС, паспортные данные, лицевой счет;
* данные о статусе студента — зачисление, отчисление, восстановление, выпуск, перевод из другого учебного заведения, перевод в другую группу, изменение вида финансирования, уход в академический отпуск и восстановление из него;
* данные о стипендиях — назначение, приостановка, продление, отмена, период назначения, дата прекращения, размер стипендий, списки студентов.

1. Этот реестр передается в банк в электронном виде.
2. Банк обрабатывает данные и осуществляет переводы на счета студентов.

Однако текущий уровень документации требует актуализации и дополнений для полного соответствия современным требованиям законодательства, стандартов и вызовам цифровой эпохи. Некоторые документы, такие как политика обработки персональных данных, регламенты работы с информационными системами, должностные инструкции сотрудников отдела ИБ и документация по обеспечению безопасности лабораторной инфраструктуры, нуждаются в доработке с учетом новых угроз и технологий.

Причины обновления документов по ИБ закрепляются следующими нормативно-правовыми документами:

* Политиками ИБ в соответствии с приказом ФНС России от 19.06.2018 N ММВ-7-6/399@ «О внесении изменений в приложение к приказу ФНС России от 25.02.2014 N ММВ-7-6/66@ «Об утверждении Концепции системы управления информационной безопасностью ФНС России» [3];
* Федеральный закон от 27.07.2006 152-ФЗ «О персональных данных» [2];
* Федеральный закон от 26.07.2017 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [4];
* ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций» от 08.08.2017 [5];
* ГОСТ ISO/IEC 27001 «Методы и средства обеспечения безопасности системы менеджмента информационной безопасности. Требования» от 30.11.2021 [6];
* Приказ № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 [7];
* локальные документы образовательного учреждения.

Актуализация документов в области ИБ необходима для обеспечения соответствия действующему законодательству РФ, которое регулярно обновляется в области требований к защите данных. Кроме того, актуализация даёт возможность внедрять современные технологии и лучшие практики в процессы обеспечения ИБ, что повышает эффективность защитных мер. Основной причиной является минимизация регуляторных рисков – штрафные санкции, судебные разбирательства и другие негативные последствия при проверках регуляторов.

Чтобы решить эти задачи системно, процесс актуализации должен включать этапы, представленные в табл. 2.

Таблица 2 – Процесс актуализации

|  |  |
| --- | --- |
| Шаг 1 | Анализ текущего состояния включает в себя выявление устаревших положений и несоответствий нормативным требованиям |
| Шаг 2 | Определение перечня документов для обновления состоит из формирования списка корректируемых документов и назначение ответственных за их доработку. |
| Шаг 3 | Разработка и корректировка изменений – процесс внесения правок с привлечением экспертов и специалистов по ИБ |
| Шаг 4 | Согласование и утверждение является финальной проверкой документов уполномоченными лицами и их официальное принятие |
| Шаг 5 | Внедрение и ознакомление сотрудников означает доведение обновлённых положений до всех лиц, имеющих доступ к конфиденциальной информации и обеспечение их исполнения |
| Шаг 6 | Мониторинг и контроль – регулярная проверка соблюдения новых требований и их эффективности на практике |

Рисунок 5 – Этапы актуализации документов

Для разработки каждого из документов необходимо определить ключевые моменты:

* область действия документа, включая перечень информации, информационных систем, компонентов информационно-телекоммуникационной инфраструктуры, подлежащих защите: определение перечня информационных систем и защищаемой информации;
* цели ЗИ для исключения утечки информации ограниченного доступа и иной конфиденциальной информации, а также предотвращение несанкционированного доступа к информационным системам и содержащейся в них информации и др.
* категории лиц, участвующих в защите информации, их обязанности (функции) и полномочия (права): руководитель оператора, структурное подразделение, специалисты по защите информации, подрядные организации;
* состав организационной системы управления деятельностью по защите информации и схему взаимодействия ее элементов.
* ответственность работников за нарушение требований к защите информации.

Перед началом работ по разработке документации необходимо определить последовательность действий, которая должна быть выстроена с учетом приоритетов и взаимосвязей между документами. На первом этапе требуется обновить Общую политику ИБ, которая станет основой для всех последующих документов. Далее следует разработать инструкции по работе с персональными данными, так как их обработка является одной из наиболее уязвимых областей. Параллельно необходимо создать должностные инструкции для сотрудников отдела ИБ, чтобы четко определить их обязанности и зоны ответственности.

Следующим шагом станет разработка политики обработки персональных данных для сайта ВУЗа, включая уведомления о сборе метаданных, что особенно важно в условиях роста онлайн-взаимодействия. Для обеспечения безопасности лабораторной инфраструктуры необходимо составить перечень оборудования и разработать положения о лабораториях, которые регламентируют порядок их использования.

Для успешной реализации всех этапов актуализации документов по ИБ необходимо распределение зон ответственности. Эффективная работа требует участия не только специалистов по ИБ, но и представителей других подразделений, поскольку вопросы ЗИ затрагивают различные аспекты деятельности организации.

Ответственность за разработку и актуализацию документов в области ИБ, как правило, распределяется следующим образом:

* руководство вуза - утверждает политики и основные документы, обеспечивает необходимые ресурсы;
* служба ИБ - разрабатывает основное содержание документов, предлагает меры защиты;
* юридический отдел - проверяет соответствие нормативным требованиям;
* отделы-владельцы процессов - предоставляют информацию о бизнес-процессах для их адекватного отражения в документах;
* кадровая служба - участвует в разработке документов, связанных с работой персонала.

Таблица 3 – Ответственные и разработчики

| **Документ** | **Ответственные** | **Привлекаемые отделы** |
| --- | --- | --- |
| Политика ИБ | Руководство вуза, отдел ИБ | Юридический, IT-отдел, администрация |
| Регламенты по ПДн | Уполномоченный по ПДн, юристы | Кадры, бухгалтерия, деканаты |
| Должностные инструкции | HR, отдел ИБ | Все подразделения |
| Технические регламенты (VPN, ПО) | IT-отдел, отдел ИБ | Лаборатории, учебные центры |

Период действия документа, порядок внесения изменений и частота его актуализации определяются уровнем значимости данного документа. Политика ИБ, являясь документом высшего уровня, подлежит обязательному пересмотру не реже одного раза в год в рамках плановой актуализации. Регламенты и процедуры, относящиеся к сфере ИБ, обновляются по мере необходимости, но не реже одного раза в два года. Инструкции и методики, регулирующие текущие процессы, корректируются оперативно при возникновении изменений в технологиях или рабочих процедурах.

Инициатором внесения изменений в политику ИБ выступает руководитель подразделения ИБ либо назначенный сотрудник, ответственный за информатизацию, выполняющий функции администратора ИБ. Окончательное утверждение обновленной редакции политики осуществляется ректором учреждения или уполномоченным лицом, издающим соответствующий приказ. Контроль за соответствием документа действующим нормативным требованиям возлагается на службу ИБ при участии юридического отдела.

Плановая актуализация настоящей политики производится ежегодно и имеет целью приведение в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации. Включает в себя комплексный анализ эффективности применяемых защитных мер, проверку соответствия актуальным законодательным нормам, таким как Федеральный закон №152-ФЗ «О персональных данных» [2], №187-ФЗ «О безопасности критической информационной инфраструктуры» [4]c, а также учет изменений в информационной инфраструктуре ВУЗа, включая внедрение новых технологических решений или переход на современные платформы обработки данных.

Внеплановая актуализация политики ИБ производится в обязательном порядке в следующих случаях:

* при изменении политики РФ в области ИБ, указов и законов РФ в области ЗИ;
* при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся ИБ;
* при происшествии и выявлении инцидента (инцидентов) по нарушению ИБ, влекущего ущерб.

Процесс обновления политики ИБ начинается с подготовки предложений по корректировке документа ответственным сотрудником, после чего проект изменений проходит согласование с заинтересованными подразделениями, включая ИТ-отдел, юридическую службу и кадровые структуры. После завершения процедуры согласования издается приказ ректора о введении в действие обновленной редакции политики. Все сотрудники ВУЗа, имеющие доступ к персональным данным или участвующие в процессах обеспечения ИБ, должны быть своевременно ознакомлены с внесенными изменениями.

Предыдущие редакции политики ИБ подлежат хранению в течение пяти лет в соответствии с установленными требованиями к документообороту учреждения.

Чтобы сделать процесс обновления документов ИБ более эффективным и менее трудозатратным, рекомендуется внедрить системные решения по автоматизации и стандартизации.

1. Стандартизация с использованием шаблонов включает в себя разработку единых шаблонов для всех типовых документов по ИБ. Использование шаблонов позволяет:

* обеспечить единообразие структуры и стиля документов;
* сократить время на согласование формата;
* минимизировать человеческий фактор при подготовке документов;
* для хранения и управления шаблонами целесообразно использовать специализированные системы документооборота, такие как SharePoint, ELMA или 1С:Документооборот.

1. Автоматизация процессов

* интеграция с HR-системами обеспечивает автоматическое обновление данных о сотрудниках;
* автоматические чек-листы и напоминания позволяют не пропускать сроки пересмотра документов;
* системы электронного документооборота позволяют настроить маршруты согласования.
* автоматизация сбора данных с помощью системы анализа данных посредством мониторинга изменений в нормативных требованиях, система может автоматически собирать данные из открытых источников и оповещать ответственных лиц [1].
* система анализа данных может анализировать данные системы контроля и управления доступом и выявлять слабые места в процессе обновления документов, задержки и прочее [1].

1. Управление версиями и изменениями

* единый реестр версий документов с указанием сроков действия;
* журнал изменений с фиксацией авторов и дат правок;
* систему учета актуальности ссылок и связанных документов.

Каждый этап разработки документов должен сопровождаться анализом текущих рисков, учетом требований отечественного законодательства и международных стандартов, в случае необходимости. Кроме того, важно вовлекать в процесс всех заинтересованных лиц: сотрудников отдела ИБ, администрацию ВУЗа, преподавателей и студентов.

Опыт ВУЗа демонстрирует, что разработка и актуализация организационно-технической документации по ИБ являются важным этапом в обеспечении защиты данных и минимизации рисков.

Ключевыми факторами успеха являются:

* системный подход к созданию документов;
* регулярное обучение сотрудников и студентов;
* актуализация документации с учетом изменений в технологиях и законодательстве;
* для других образовательных учреждений данный опыт может стать основой для построения эффективной системы ИБ.

СПИСОК ЛИТЕРАТУРЫ

1. Пителинский К.В., Плоткин А.С., Кривоногов А.А. О некоторых методах и средствах развития и защиты ресурсов вуза, обеспечивающих непрерывность его деятельности // Информационная безопасность. – 2024. – № 4. – С. 15–20.
2. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 29.12.2022) «О персональных данных». – [Электронный ресурс]. – Режим доступа: <https://www.consultant.ru/document/cons_doc_LAW_61801/>, свободный. – Дата обращения: 08.05.2025.
3. Приказ ФНС России от 19.06.2018 № ММВ-7-6/399@ «Об утверждении форматов представления документов в электронном виде». – [Электронный ресурс]. – Режим доступа: <https://sudact.ru/law/prikaz-fns-rossii-ot-19062018-n-mmv-7-6399/prilozhenie/3/3.2/3.2.1/>, свободный. – Дата обращения: 08.05.2025.
4. Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 10.03.2023) «О безопасности критической информационной инфраструктуры Российской Федерации». – [Электронный ресурс]. – Режим доступа: <https://www.consultant.ru/document/cons_doc_LAW_220885/>, свободный. – Дата обращения: 08.05.2025.
5. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации. Общие положения. – [Электронный ресурс]. – Режим доступа: <https://itglobal.com/wp-content/uploads/2021/05/gost-57580.1-1.pdf>, свободный. – Дата обращения: 08.05.2025.
6. ГОСТ Р ИСО/МЭК 27001-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью. Требования. – [Электронный ресурс]. – Режим доступа: <https://docs.cntd.ru/document/1200181890>, свободный. – Дата обращения: 08.05.2025
7. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». – [Электронный ресурс]. – Режим доступа: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21>, свободный. – Дата обращения: 08.05.2025.