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

*Аннотация: Статья посвящена комплексному подходу к созданию и обновлению организационно-технической документации в сфере информационной безопасности на примере университета. В материале рассматриваются ключевые документы, такие как инструкции по работе с персональными данными, политики обработки данных, должностные инструкции для сотрудников отдела информационной безопасности, а также технические регламенты и положения о лабораториях. Особое внимание уделяется актуализации существующих документов, таких как Общая политика информационной безопасности, 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.*

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

На первом этапе разрабатывается и утверждается политика защиты информации, 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 защиты информации. 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.

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 таблице 1.

Таблица 1 – Примеры внутренних стандартов и регламентов

|  |  |
| --- | --- |
| **Внутренние стандарты** | Требования к обновлению программного обеспечения |
| 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 защиты информации |
| Регламент управления учетными записями |
| Порядок тестирования знаний по вопросам информационной безопасности. |
| Регламенты передачи данных |

Информационная безопасность (ИБ) является одной из ключевых задач для образовательных учреждений, особенно в условиях цифровой трансформации.

Так как Университеты сталкиваются с необходимостью защиты персональных данных студентов, сотрудников, научных разработок и других конфиденциальных сведений, на сегодняшний день в университете ведется активная работа по совершенствованию системы организационно-технической документации в области ИБ.

В случае наличия у университета филиалов в других городах необходимо учитывать особенности передачи конфиденциальной информации по телекоммуникационным сетям. 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.
2. Этот реестр передается в банк в электронном виде.
3. 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.

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 информационной безопасности, 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.

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 защиты информации 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 о защите информации.

Следующим шагом станет разработка политики обработки персональных данных для сайта университета, 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.

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 университета, преподавателей и студентов.

Опыт университета демонстрирует, что разработка и актуализация организационно-технической документации по информационной безопасности 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 информационной безопасности.