Обеспечение безопасности информации – это неотъемлемая составляющая успешной работы в онлайн-мире. Это комплексная система мер, направленных на обеспечение непрерывной работы сайта, а также на защиту конфиденциальности, целостности и доступности хранимой на нем информации для пользователей.

Для создания стабильного сайта для АНО «Центр Единство», исправно выполняющего функции, необходимо проанализировать, какие аспекты продукта подвержены угрозам. Уже на основе полученных данных определяются способы обеспечения безопасности разрабатываемого веб ресурса.

Сайт предназначен для хранения и/или передачи следующей информации:

1. ФИО или имя, номер телефона и email человека, который оставил просьбу на сайте с помощью формы обратной связи. Полученные данные отправляются администратору – сотруднику заказчика по почте для дальнейшего контакта отправителем, и позже удаляются;
2. Учредительные документы и отчеты о деятельности организации;
3. Статьи о завершенных проектах и событиях в жизни организации.

Особое внимание необходимо уделить данным из первого пункта списка, т. к. они являются персональными и взаимодействие с ними регламентируется Федеральным законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных».

Утечка или повреждение перечисленных данных может привести к серьезным последствиям и принести ущерб репутации организации заказчика. Помимо вышеописанных угроз, причинами нарушения целостности и безопасности могут стать факторы, перечисленные в таблице НН.

Таблица НН – Модель угроз безопасности сайта АНО «Центр Единство»

|  |  |
| --- | --- |
| ВНУТРЕННИЕ | - Риск непреднамеренного изменения или повреждения данных, размещаемых на сайте, администратором – сотрудником заказчика;  - Риск преднамеренного изменения или повреждения размещаемых данных администратором с целью нанесения ущерба репутации организации, распространения компьютерных вирусов посредством документов;  - Риск использования данных, отправленных с сайта посредством формы в целях, иных от контакта с обратившимся человеком для обеспечения дальнейшей поддержки. |
| ВНЕШНИЕ | - Несанкционированный доступ лиц не являющимися администраторами данного сайта и/или сотрудниками организации заказчика;  - Угроза хакерских атак с целью нарушения стабильной работы сайта, целостности хранимых данных, их хищения и/или причинения ущерба репутации организации. |
| ТЕХНИЧЕСКИЕ | - Нарушение целостности данных вследствие сбоев веб-хостинга; |

Для обеспечения безопасности используются следующие методы:

1. Разграничение доступа к информационным системам. Разграничение доступа — это комплекс правил, который определяет для каждого субъекта, метода и объекта наличие или отсутствие прав доступа к объектам или данным с помощью указанного метода.

Разграничение доступа к сайту реализуется встроенными средствами Django REST Framework. Аутентификация поддерживает различные методы аутентификации, такие как базовая аутентификация, аутентификация по токенам, OAuth2. Это позволяет верифицировать личность пользователей и предоставлять доступ только авторизованным лицам. Авторизация: DRF предоставляет механизмы для определения прав доступа на уровне объектов и действий. Можно использовать встроенные разрешения или создавать собственные, чтобы ограничить доступ пользователей к определенным данным или функциям.

1. Резервное копирование данных (бэкап). Использование резервного копирования позволяет создавать копии файлов на другом устройстве или в облачной инфраструктуре для быстрого восстановления данных в случае утери или повреждения носителя.

Резервное копирование данных реализуется с помощью инструментов, предоставляемых виртуальным хостингом, на котором будет размещен сайт.

1. Защита от утечек данных. Защита от утечек данных - это реализация комплекса мер, которые направлены на то, чтобы обеспечить сохранность и целостность конфиденциальной информации организации для уменьшения вероятности возникновения финансовых и репутационных потерь, если произойдёт утечка.

Для предотвращения утечек данных, используется:

* Валидация данных: DRF предоставляет средства для валидации входных данных, предотвращая SQL-инъекции и другие виды атак, связанные с недоверенными данными;
* HTTPS: Использование HTTPS для шифрования трафика между клиентом и сервером защищает данные от перехвата;
* Хеширование паролей:  Пароли хранятся в захешированном виде, используя алгоритмы bcrypt или PBKDF2, предотвращая их расшифровку в случае компрометации базы данных;
* Протоколирование и аудит. Протоколирование - это процесс сбора и накопления информации о тех событиях, которые происходят в информационной системе предприятия. Аудит – анализ накопленной информации, проводимый в режиме реального времени или с определенной периодичностью.

Также обеспечение информационной безопасности включает в себя регулярное обновление программного обеспечения и проведение профилактических мероприятий для приложений. Это позволяет закрывать уязвимости, которые могут быть использованы злоумышленниками для атак на сайт, и обеспечивает его защиту от различных видов киберугроз.

Еще одним важным аспектом является контроль за целостностью данных с помощью специальных скриптов. Поскольку даже небольшие ошибки в коде сайта могут привести к нарушению целостности данных, необходимо периодически проверять их на наличие дефектов или изменений, которые могли возникнуть в результате злонамеренных действий.