5 ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для обеспечения информационной безопасности разрабатываемой системы необходимо достичь следующих целей безопасности:

- Разрабатываемая система должна обладать механизмами регистрации любых событий, относящихся к возможным нарушениям безопасности.
- Необходимо обеспечить управление параметрами системой антивирусной защиты.
- Управление системной антивирусной защиты должно быть доступно только уполномоченным группам лиц.
- Доступ к системе должен быть ограничен в соответствии с ролями пользователей в системе.
- В системе должны быть реализованы регулярные проверки с целью обнаружения файлов, зараженных компьютерными вирусами.
- В антивирусном программном обеспечении должна быть реализована обработка зараженных файлов.
- База данных антивирусного ПО должна регулярна обновляться и содержать актуальную информацию о списке существующих компьютерных вирусов.

Кроме того, организация информационной безопасности разрабатываемой системы подразумевает наличие у объекта следующих свойств:

- разрабатываемая ИАС должна иметь доступ ко всем объектам, которые необходимы для функционирования системы;
- должны быть обеспечены установка и управление разрабатываемой системой в соответствии с правилами эксплуатации;
- должна быть обеспечена физическая защита компонентов системы, на которых установлена ИАС, а также хранятся данные, необходимые для функционирования системы;

- взаимодействия между элементами системы должны быть синхронизированы по времени;
- для взаимодействий между элементами системы должны использоваться доверенный каналы связи, обеспечивающие конфиденциальность передаваемых данных;
- лица, обеспечивающие функционирование разрабатываемой ИАС, обязаны обеспечивать функционирование системы в соответствии с установленной документацией.

Для обеспечения вышеперечисленных свойств необходимо рассмотреть возможные уязвимости и угрозы, которым необходимо противостоять в рамках реализации информационной безопасности системы.

5.1 Анализ уязвимостей и угроз для разрабатываемой ИАС

Для разрабатываемой информационной системы характерны следующие группы угроз:

- угрозы, которым должна противостоять разрабатываемая система;
- угрозы, которым должна противостоять среда, в рамках которой функционирует ИАС.

При рассмотрении первой группы угроз, были выявлены следующие опасности для разрабатываемой системы.

Угроза получения несанкционированного доступа к данным. Источником данной угрозы является внешний нарушитель. Реализация данной угрозы возможна путем получения нарушителя доступа к файлам cookie. Уязвимостью для возможности реализации данной угрозы являются недостатки реализации компонента аутентификации пользователей. При этом нарушаются такие свойства безопасности системы как конфиденциальность и целостность. Последствиями реализации данной угрозы является утечка, изменение или удаление конфиденциальных данных пользователя.

Угроза перехвата передаваемых данных. Возможность реализации данной угрозы обусловлена передачей данных по незащищенному каналу связи. Для

реализации данной угрозы нарушитель может воспользоваться недостатками компонента шифрования разрабатываемой аналитической системы. Наличие данной уязвимости приводит к нарушению конфиденциальности и представляет угрозу для данных пользователя.

К рассмотренным угрозам также относится угроза подмены web-сайта. Данная угроза может быть реализована в случае, если используется протокол HTTP и отсутствует сертификат SSL. Реализация данной угрозы может привести к тому, что данные, передаваемые пользователем, будут переданы на сторонние ресурсы, тем самым будут нарушены свойства системы, такие как конфиденциальность и целостность.

Кроме того, были рассмотрены угрозы, которым должна противостоять среда, в которой функционирует разрабатываемая система. К таким угрозам можно отнести внедрение компьютерного вируса в устройство, на котором развернута ИАС и хранится база данных. Данная угроза реализуема в виду отсутствия или наличия неполного комплекса средств защиты информации в информационной системе. Ресурсами, подверженными угрозе, в данном случае являются конфиденциальная информация пользователей, хранящаяся в базе данных, файлы самой информационный системы и т.д. При реализации данной угрозы будут нарушены такие свойства системы как целостность, конфиденциальность и доступность. Последствиями угрозы являются утечка конфиденциальной информации и нарушение функционирования разрабатываемой ИАС.

Также существует угроза DDoS-атаки разрабатываемой системы. Данная угроза реализуется через уязвимости в настройках сервера. При реализации данной угрозы ресурс перегружается запросами и становится недоступным для использования, тем самым нарушается доступность системы. Последствиям реализации данной угрозы становится отказ пользователям в доступе к системе.

5.2Реализация средств обеспечения безопасности в клиентских приложениях

Для предотвращения угрозы перехвата данных в разрабатываемой системе реализован модуль шифрования. Перед передачей информации данные шифруются, а после получения расшифровываются для последующей обработки (рисунок 5.1). При этом данные по сети передаются в зашифрованном виде, тем самым, при перехвате данных, злоумышленник не сможет получить информацию.

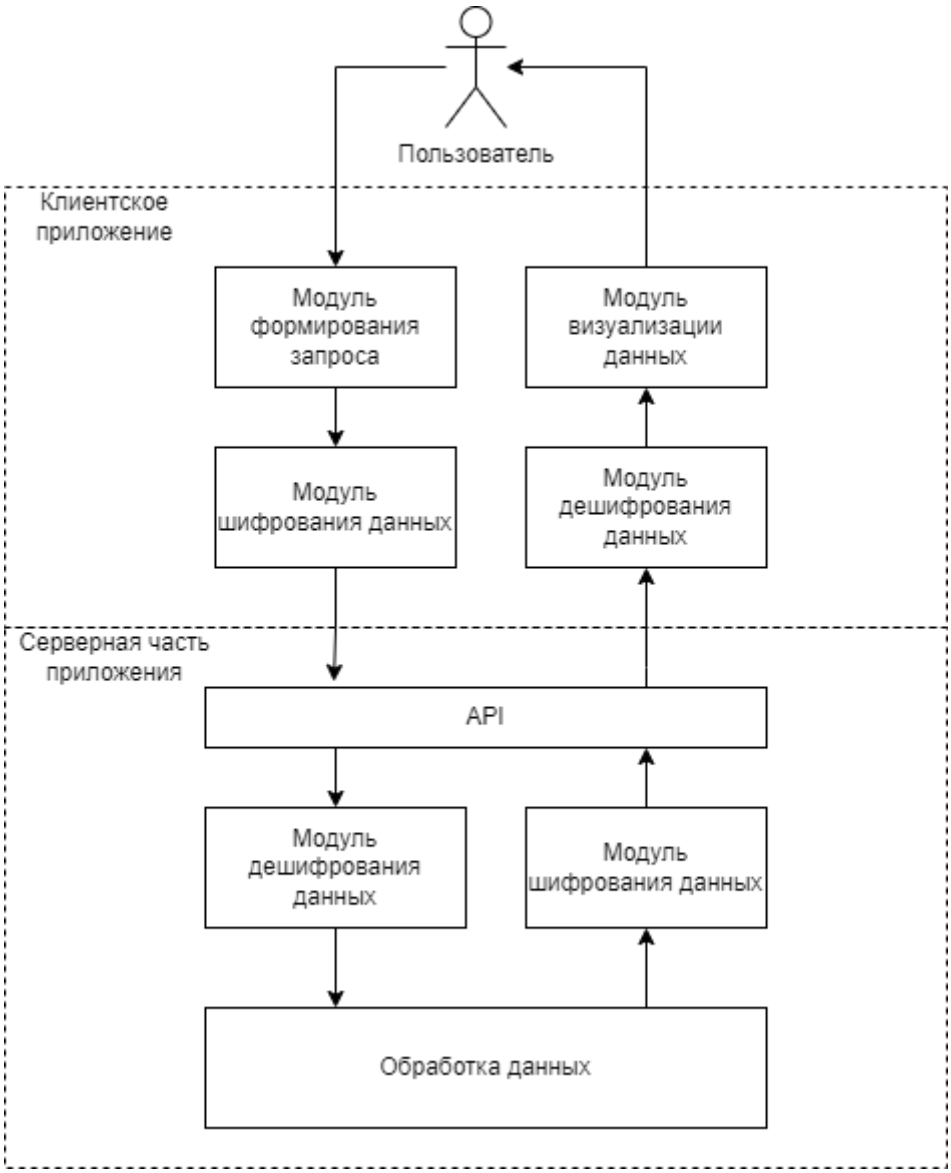

Рисунок 5.1 – Алгоритм передачи данных между клиентским приложением и сервером

Так как пользователь может взаимодействовать с системой посредством браузера, то и на этом уровне должна быть обеспечена защита передаваемых данных. Однако, встроить модули шифрования в программный код браузеров не является возможным. Поэтому в разрабатываемой системе применяется протокол HTTPS. Протокол обеспечивает шифрование данных между пользователем и сервером. Кроме того, использование этого протокола позволяет реализовать защиту от угрозы подмены контента web-сайта. Получение SSL-сертификата реализовано с помощью сервиса Let's Encrypt.

В качестве дополнительного механизма защиты применяется технология HSTS. Суть технологии заключается в том, что браузеру передается защищенный заголовок HTTP Strict Transport Security, после чего браузер автоматически будет обращаться к ресурсу по протоколу HTTPS, а соединение с использованием протокола HTTP перестает обслуживаться.

Многие старые версии браузеров не могут обеспечить безопасность данных в достаточной мере. В виду этого, при разработке ИАС, было принято решение реализовать запрет на использование системы в устаревших версиях браузеров, которые не соответствуют современный нормам обеспечения информационной безопасности. Кроме того, на сервере используются последние версии программного обеспечения, что позволяет использовать актуальные средства защиты информации.

Также, для обеспечения информационной безопасности на программном уровне ИАС разрабатывалась в соответствии с правилами объектно-ориентированного программирования. В их число входит обеспечение такого свойства как инкапсуляция, благодаря чему в программном коде исключается передача скрытых данных в зону видимости пользователя. Это исключает возможное раскрытие конфиденциальной информации.

5.3 Реализация средств обеспечения безопасности в серверных приложениях

Для обеспечения информационной безопасности на серверной части разрабатываемого продукта реализованы такие компоненты, как модуль логирования, модуль шифрования и дешифрования сессии и модуль авторизации.

Модуль логирования необходим для сохранения информации о работе разрабатываемой ИАС. Наличие лог-файлов позволяет администратору или программисту быстрее определять неисправности и уязвимости системы для их предотвращения. Также анализ лог-файлов позволяет определить перечень действий, которые могли привести к некорректному поведению программного продукта, или вычислить и заблокировать доступ нарушителю, желающему навредить работе аналитической системы.

Реализованный модуль авторизации позволяет ограничить доступ пользователей к системе. Данный модуль решает проблему несанкционированного доступа к конфиденциальной информации. Доступ организуется посредством ввода логина и пароля. Логин и пароль хранятся в базе данных, при это пароль подвергается хешированию. То есть пароли в базе данных не хранятся в открытом виде, что гарантирует обеспечение конфиденциальности даже в случае получения злоумышленником доступа к базе данных.

В случае получения нарушителем доступа к файлам cookie пользователя, нарушитель может получить доступ к личному кабинету пользователя. Для предотвращения данной угрозы в программный код разрабатываемого продукта внедрена дополнительная проверка данных браузера и IP-адреса пользователя.

В виде базового средства обеспечения безопасности на сервере в качестве операционной системы используется Linux Ubuntu 22.04 LTS. Выбор в пользу Linux был сделан, потому что большинство существующих вирусов

ориентированы на Windows, также в Linux реализовано четкое разделение привилегий пользователей.

В качестве межсетевого экрана на сервере используется утилита iptables. Данная утилита с помощью установленных правил контролирует входящие и исходящие пакеты данных, а также в зависимости от правил при необходимости блокирует трафик.

Для подключения к серверу используется протокол SSH, это обеспечивает шифрование сеанса связи с сервером. Кроме того, для подключения к серверу необходимо пройти этап двухфакторной аутентификации. Данный механизм реализован с помощью модуля Google Authenticator PAM. Благодаря чему кроме имени пользователя и пароля, требуется дополнительно ввести генерируемый верификационный код. Данная реализация гарантирует сохранение конфиденциальности данных, даже в случае рассекречивания логина и пароля для подключения к серверу.

На сервере настроены ежедневные бэкапы данных, при этом данные сохраняются как в локальном, так и в облачном хранилище. Это необходимо, чтобы в случае ЧП можно было быстро восстановить утерянные данные. Бэкап серверных файлов осуществляется при помощи утилиты gnome-disk-utility, резервное копирование база данных осуществляется средствами СУБД. Важным в данном случае является хранение удаленных резервных копий в облачном хранилище, при это передача данных происходит с применением шифрования.

В качестве дополнительных средств обеспечения безопасности системы на сервере используется специальное программное обеспечивание. В случае кражи носителя данных с сервера необходимо предусмотреть защиту от утечки данных, для шифрования файлов на сервере используется VeraCrypt 1.25.9. Плюсами данной программы является возможность шифрования диска сервера с использованием алгоритма шифрования «Кузнечик» и алгоритма вычисления хэш-функции «Стрибог».

Для управления базой данных на сервере установлена СУБД MySQL Server 8.0.29. Данная система поддерживает шифрование по алгоритму AES-256, благодаря чему существует возможность обеспечить защиту полей базы данных от несанкционированного доступа.

В качестве антивирусного ПО используется ESET NOD32 Antivirus Business Edition. Данное ПО входит в список лучших средств антивирусной защиты для серверов. Выбранный антивирус входит в государственный реестр сертифицированных средств защиты информации ФСТЭК России.

Также важным аспектом обеспечения информационной безопасности серверной части разрабатываемой системы является использование последних версий программного обеспечения. Это необходимо, так как старые версии приложений могут иметь уязвимости, влияющие на безопасность работы ИАС.

Также стоит отметить, что угроза доступа к конфиденциальной информации пользователей системы может быть реализована путем внедрения компьютерного вируса на персональные устройства пользователя. Однако в данном случае ответственность за утечку данных несет сам пользователь.

5.4 Технические средства обеспечения безопасности

Технические средства необходимы для обеспечения таких свойств системы, как доступность, целостность и конфиденциальность.

Для защиты сервера от несанкционированного доступа, серверное оборудование располагается в специально оборудованном помещении, с ограниченным доступом. Для защиты от проникновения в данное помещение использована защитная дверь с запирающим механизмом, также помещение оснащено защитной сигнализацией.

При этом в помещении обеспечена постоянная поддержка оптимальной температуры воздуха, что реализуется установленным кондиционером. Кроме того, серверное помещение оборудовано системой автоматического пожаротушения.

Для обеспечения постоянной доступности ресурса, сервер обеспечен резервным источником питания, наилучшим решением является использование источников бесперебойного питания (ИБП). Также для обеспечения доступности ресурса через интернет сервер можно обеспечить резервным каналом связи, и в случае неполадок в работе основного канала связи, провайдер сможет переключить сервер на резервный канал.

5.5 Описание организационных мер обеспечения безопасности

Для обеспечения безопасности системы разработана политика безопасности, которая включает в себя следующие правила:

- Должна быть разработана внутренняя документация, включающая правила работы с разрабатываемой системой.
- Должен быть составлен алгоритм действий, применяемых в случае выхода сервера из строя.
- Необходимо производить инструктаж персонала об ответственности за разглашение конфиденциальной информации.
- Должна быть реализована регистрация любых событий, относящихся к нарушениям безопасности.
- Настройка антивирусного программного обеспечения должна осуществляться только уполномоченными субъектами системы.
- Должна быть обеспечена защита от несанкционированного доступа к данной разрабатываемой ИАС.
- Должна быть обеспечена регулярная проверка файлов и областей памяти с целью обнаружения объектов, зараженных компьютерными вирусами.
- Должна быть обеспечена возможность изоляции и удаления файлов, зараженных компьютерными вирусам.
- В системе антивирусного программного обеспечения должно быть реализовано автоматическое обновление базы данных компьютерных вирусов.