ОСОБЕННОСТИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ НЕСОВЕРШЕННОЛЕТНИХ В СЕТИ ИНТЕРНЕТ В РОССИЙСКОЙ ФЕДЕРАЦИИ

В.С. Беззатеева, *Санкт-Петербургский государственный университет аэрокосмического приборостроения, bezzateeva@inbox.ru.*

УДК 004.056

Аннотация. Статья посвящена актуальной проблеме защиты несовершеннолетних в сети Интернет, в исследовании представлен комплекс мер и технологий, направленных на обеспечение информационной безопасности данной возрастной категории. Рассматриваются современные технологии фильтрации контента с использованием баз данных вредоносных и нежелательных сайтов, а также технологии машинного обучения для выявления опасных ресурсов. Описаны механизмы реализации мониторинга активности несовершеннолетних, времени пребывания онлайн, контроля доступа и аутентификации, также раскрыты основополагающие аспекты криптографической защиты.

Ключевые слова: защита несовершеннолетних; контент-фильтрация; *HSM*-шифрование; кибербезопасность.

FEATURES AND PROSPECTS OF DEVELOPMENT OF TECHNICAL SUPPORT FOR THE SAFETY OF MINORS ON THE INTERNET IN THE RUSSIAN FEDERATION

V.S. Bezzateeva, *Saint-Petersburg State University of Aerospace Instrumentation.*

Annotation. The article is devoted to the actual problem of protecting minors on the Internet. The study presents a set of measures and technologies aimed at ensuring information security for this age group. It examines modern technologies for filtering content using databases of malicious and unwanted websites, as well as machine learning technologies for identifying dangerous resources. The article describes the mechanisms for monitoring the activity of minors, their online time, access control, and authentication, and reveals the fundamental aspects of cryptographic protection.

Keywords: protection of minors; content filtering; HSM encryption; cybersecurity.

Введение

В силу развития сети Интернет и цифровизации общества в целом, на сегодняшний день особенно актуальной становится проблема защиты несовершеннолетних, как наиболее уязвимой категории пользователей, от различного рода нежелательной информации и необдуманных действий в цифровом информационном поле. Нормативно-правовые акты Российской Федерации предусматривают ответственность за размещение вредоносного контента, подстрекательство к противоправным и аддиктивным действиям, кражу персональных данных. На сегодняшний день реализуется инициатива внедрения детских сим-карт, которые дадут возможность разграничения контента по возрастной категоризации и предотвращения противоправных действий со стороны злоумышленников в отношении несовершеннолетних. В Российской Федерации в настоящее время особое внимание уделяется обеспечению безопасности несовершеннолетних в сети Интернет посредством комплекса технических мер.

Среди наиболее распространенных мер защиты используются:

- режим «родительский контроль и трекинг владельца телефона»;
- программно настраиваемый фильтр контента;
- антивирусные программы и системы обнаружения угроз;
- программы блокировки доступа к запрещенным ресурсам (по решению государственных органов);
- системы мониторинга и анализа трафика;
- мобильные приложения и браузеры со встроенными средствами защиты, предназначенные для безопасного серфинга несовершеннолетних [1-3].

Безопасная среда в образовательном учреждении подразумевает наличие школьных информационных систем, оснащенных средствами фильтрации и контроля доступа, а также программы обучения учащихся правилам и навыкам безопасного поведения в сети Интернет и использованию программно-технических средств защиты. Нормативно-правовая база Российской Федерации, направленная на обеспечение безопасности несовершеннолетних в сети Интернет, включает в себя Федеральный закон №152-ФЗ «О персональных данных» от 27 июля 2006 г.[1], Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»[2], Федеральный закон от 24 июля 1998 г. N 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»[3].

Пути развития программно-технических средств защиты несовершеннолетних в сети Интернет.

Среди перспективных направлений развития программно-технических средств защиты можно выделить создание архитектуры системы, построенной на принципах комплексной, многоуровневой защиты, включающей фильтрацию контента, контроль доступа, шифрование данных и мониторинг активности, подразумевающей, в том числе, анализ поведения пользователя с выявлением нестандартных, не свойственных ему поведенческих элементов. В случае интеграции такой системы в локальную сеть необходима установка ее элементов на маршрутизаторе или отдельном сервере, обеспечивающем фильтрацию и контроль.

Компоненты системы включают в себя:

А) Модуль фильтрации контента, который подразумевает использование публичных и коммерческих списков вредоносных и нежелательных сайтов (*OpenDNS, Cisco Talos*, списки Центра безопасного интернета в России, списки Лаборатории Касперского, собственные базы данных) и регулярное обновление через *API* или автоматические скрипты; анализ *URL*, заголовков страниц, метаданных для фильтрации контента по ключевым словам и категоризации (насилие, порнография, азартные игры) – актуальным является использование

---

[1] Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» URL: https://www.consultant.ru/document/cons_doc_LAW_61801 (дата обращения: 01.11.2025).

[2] Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 N 436-ФЗ URL: https://www.consultant.ru/document/cons_doc_LAW_108808 (дата обращения: 01.11.2025).

[3] Федеральный закон "Об основных гарантиях прав ребенка в Российской Федерации" от 24.07.1998 N 124-ФЗ URL: https://www.consultant.ru/document/cons_doc_LAW_19558 (дата обращения: 01.11.2025).

регулярных выражений и классификаторов на базе машинного обучения; реализация машинного обучения посредством обучения моделей на наборах данных вредоносных и опасных сайтов и анализе содержимого страниц в реальном времени с помощью *API* (*Google Clod Vizion, ScraperAPI, Azure Cognetive Services*); техническая реализация на основе встроенного прокси-сервера или *DNS*-сервера, перехватывающих запросы, и использование фильтрующих движков (*Squid, DansGuardian*) [4, 5]. Кроме того, сюда же входит использование решений, которые анализируют поведение ребенка в сети Интернет и автоматически адаптируют ограничения (например, системы, подобные *Qustodio* или *Bark*).

Б) Модуль контроля доступа и ограничения времени использования интернета при помощи ограничения по *IP, URL*, категориям, а также установление временных рамок (например, доступ только в интервале с 17:00 до 20:30 час.), возможно посредством использования встроенных функций маршрутизатора или отдельного сервера (*firewalld*, на базе *Linux с iptables, cron*) и использования веб-интерфейса для настройки правил [6].

В) Модуль шифрования и защиты данных – использование протоколов *TLS* 1.3 для всех соединений или внедрение *VPN*-сервиса для защиты всего трафика.

Шифрование локальных данных происходит при помощи хранения логов и персональных данных в зашифрованном виде [7]. Целью является обеспечение конфиденциальности и целостности данных, предотвращение несанкционированного доступа при физическом или удаленном взломе системы. Технология, использующая отечественный стандарт шифрования «Кузнечик» (ГОСТ Р 34.12-2015) – один из наиболее надежных и рекомендованных к использованию на территории РФ алгоритмов симметричного шифрования.

Процесс шифрования:

- Генерация ключа с помощью криптографически стойкого генератора случайных чисел. Дальнейшее хранение ключа в защищенной области, например, в аппаратных модулях *Hardware Security Module* (*HSM*) или в защищенной части системы, например, *Trusted Platform Module* (*TPM*).
- Шифрование данных с помощью симметричного алгоритма в режиме *Gaios/Counter Mode (GCM)* перед сохранением логов или персональных данных для обеспечения шифрования и аутентификации данных.
- Расшифрование данных при необходимости доступа к информации осуществляется с помощью того же ключа.
- Обеспечение безопасности ключей гарантируется тем, что ключи не хранятся в открытом виде в системе и используются механизмы защиты ключей, такие как *HSM* или *TPM*.

Шифрование с помощью *HSM* подразумевает создание ключей внутри *HSM*, что исключает их кражу или копирование, внутри *HSM* ключи хранятся в зашифрованном виде и недоступны для внешних систем [8, 9]. Для шифрования или расшифровки данных система отправляет запросы к *HSM* через защищенный интерфейс, *HSM* выполняет криптографические операции, возвращая зашифрованные или расшифрованные данные. Все операции с ключами и данными регистрируются в журнале внутри *HSM*, и тут возможна настройка автоматического аудита и контроля доступа.

Таким образом, генерация ключа происходит внутри *HSM*, журналы и персональные данные шифруются с помощью надежного симметричного алгоритма в режиме *GCM*, используя ключ, хранящийся в *HSM*. Доступ к зашифрованным данным осуществляется только через запросы к *HSM*, что

исключает возможность кражи ключа и при необходимости анализа или просмотра данных – они расшифровываются внутри *HSM*, а результат передается системе в зашифрованном виде. Также необходимо предусмотреть внедрение сквозного шифрования (*End-to-End Encryption, E2EE*) для всех передаваемых данных и использование технологии блокчейн для хранения логов активности, чтобы обеспечить их низменность и безопасность [10].

Г) Модуль аутентификации и авторизации подразумевает наличие родительского контроля, т.е. внедрение системы аутентификации несовершеннолетнего через учетную запись родителей и использование биометрических данных (например, отпечаток пальца, венозный рисунок ладони или распознавание лица) для доступа к настройкам [11]. Реализация возможна посредством интеграции с платформами аутентификации или мобильными приложениями/веб-интерфейсами для управления.

Д) Модуль оповещения и мониторинга – реализация системы ведения журнала и анализа активности при помощи записи всех запросов, списка посещенных сайтов, времени доступа и хранения логов в зашифрованном виде. И последующие автоматические уведомления родителей, учителей или других ответственных лиц по электронной почте или через мобильное приложение при обнаружении подозрительной активности или попытках доступа к запрещенным ресурсам.

Интеграция системы защиты несовершеннолетнего в сети Интернет включает в себя следующие обязательные составляющие:

1. Централизованное управление – обеспечение единого интерфейса для настройки и мониторинга посредствами панели управления, облачных платформ.

2. Регулярное автоматическое обновление фильтров, программных компонент и системы оповещения.

Особую актуальность и интерес с точки зрения эффективности работы представляют собой системы анализа поведения пользователя при работе с мобильным устройством (смартфоном) или планшетом, ноутбуком, стационарным персональным компьютером. Благодаря тому, что поведенческие особенности пользователя в целом сохраняются и практически не зависят от используемого им устройства, такой механизм позволяет идентифицировать пользователя и не требует при этом сложной, с организационной точки зрения, процедуры его идентификации и аутентификации. Кроме того, такая система не заметна для пользователя и, соответственно, не вызывает желания ее обойти каким-либо образом. В особенности это относится именно к категории несовершеннолетних пользователей. В Российской Федерации программно-технические системы, позволяющие реализовывать поведенческую аутентификацию пользователя, только начинают разрабатываться, несмотря на наличие существенного теоретического базиса. Безусловно, за такими системами большое будущее, особенно в случае подключения систем искусственного интеллекта и создания больших наборов данных для обучения соответствующих моделей нейронных сетей.

Другой не менее актуальной проблемой в настоящее время можно считать задачу надежной аутентификации аудио, видео и текстовой информации, поступающей на коммуникационное устройство (смартфон, ноутбук, настольный компьютер) пользователя. Ввиду активного развития моделей искусственного интеллекта и совершенствования систем, успешно манипулирующих с различным контентом для создания цифровых двойников и реализации с их помощью различных фейковых структур (аудио, видео, текст) во многих случаях для неподготовленного пользователя в экстремальных психоэмоциональных условиях

практически неотличимых от реальных людей, знакомых и близких несовершеннолетнему. Возможным решением такой проблемы является использование электронной цифровой подписи для текстовых сообщений и соответствующих цифровых водяных знаков для аудио и видео информации.

Для реализации имеющихся и хорошо проверенных в теории алгоритмов, обеспечивающих такую аутентификацию, необходимо создание соответствующего программного обеспечения и технической базы для его эффективной реализации. При этом существенной проблемой для успешной реализации такой защиты является наличие на устройстве учащегося постоянно обновляемой базы сертификатов, позволяющих проверить достоверность (аутентичность) получаемой информации. Однако в случае защиты несовершеннолетнего от эмоционально-психологического воздействия посторонних, поддельных источников информации такая задача достаточно легко решается вследствие ограниченного круга лиц, которые имеют право отправлять критически важную информацию такому получателю. Круг таких лиц ограничивается учителями, воспитателями, родителями, лицами, выполняющими функции опекунства и т.д. [12].

Общая архитектура схемы технической реализации системы защиты несовершеннолетнего выглядит следующим образом:

- клиентское устройство (ПК, смартфон, планшет) использует установленное приложение или встроенные средства для доступа к сети Интернет, взаимодействуя с системой через защищенный канал (*VPN, TLS*);
- локальный шлюз/маршрутизатор с интегрированным фильтром и шифровальщиком перехватывает все запросы и трафик, выполняя функцию фильтрации контента и контроля доступа, далее передает данные для шифрования и хранения;
- сервер системы защиты обрабатывает запросы на шифрование/ расшифрование, взаимодействуя с *HSM* для генерации и хранения ключей и в дальнейшем хранит логи и персональные данные;
- аппаратный модуль безопасности (*HSM*) генерирует, хранит и управляет криптографическими ключами, выполняет операции шифрования и расшифровки по запросу сервера, таким образом, обеспечивая высокий уровень защиты ключей и данных.

Заключение

Предложенная архитектура системы защиты несовершеннолетних в сети Интернет способствует созданию надежной инфраструктуры для защиты данной возрастной категории пользователей, обеспечивая баланс между удобством использования технических устройств и минимизацией рисков, связанных с несанкционированным доступом к потенциально опасному контенту, аддиктивным воздействием и использованием персональных данных.

Таким образом, внедрение предложенных решений позволит значительно увеличить уровень защищенности несовершеннолетних в сети Интернет, обеспечив здоровое развитие подрастающего поколения и минимизировав риски, связанные с использованием цифрового пространства.

Литература

1. Ушкин С.Г., Коваль Е.А., Мартынова М.Д. Цифровая безопасность подростков: социологический анализ // Интеграция образования, 2025. – Т. 29. – № 1. – С. 114-131.

2. Назаров М.М. Приватность в сети и цифровая покорность: исследование аудитории интернет // Вестник Института социологии, 2022. – Т. 13. – № 3. – С. 87-107.
3. Ганский П.Н. Интернет-пространство как особая коммуникационная среда и его влияние на современное общество. – URL: https://docviewer.yandex.ru/view/475640418/ (дата обращения: 01.11. 2025).
4. Колесникова Д.С. Применение систем контентной фильтрации в образовательных учреждениях для защиты детей от нежелательной информации // Молодой ученый, 2017. – № 7 (141). – С. 20-22.
5. Апетьян С.Д., Ковалев А.А., Файб А.Б. Фильтрация контента в Интернете. Анализ мировой практики. – URL: http://civilfund.ru/Filtraciya_Kontenta_V_Internete_Analiz_Mirovoy_Praktiki.pdf (дата обращения: 03.11.2025).
6. Гатченко В.О. Контроль за использованием средств связи и сети интернет в условиях домашнего ареста: вызовы и решения // StudArctic forum, 2024. – Т. 9. – № 1. – С. 56-64.
7. Бакаева О.А., Барабошкин Д.А. Разработка протокола передачи данных на основе комбинированного алгоритма их щифрования // Программные продукты и системы, 2023. – Т. 36 – № 3 – С. 493-499.
8. Жестков, А.Д. Способы хранения закрытых ключей и будущее технологии HSM // Молодой ученый, 2024. – № 2. – С. 1-14.
9. Микаева А.С. Внутренняя структура сервиса управления криптографическими ключами – URL: https://dnevniknauki.ru/images/publications/2022/12/technics/Mikaeva_Nikolaev.pdf (дата обращения: 01.11.2025).
10. Позняк П.П. Сквозное шифрование или end-to-end encryption (E2EE) в мессенджерах // 74-я научно-техническая конференция учащихся, студентов и магистрантов: тезисы докладов, 17-22 апреля 2023г., Минск: БГТУ, 2023. – Т. 4 – № 4. – С. 249-251.
11. Заярная И.А., Петрич А.Р. Аутентификация: теоретические аспекты // Вестник Алтайской академии экономики и права, 2022. – № 10-3. – С. 416-420.
12. Беззатеева В.С. Использование идентификационной карты для защиты несовершеннолетнего от деструктива и других угроз в сети Интернет // Социотехнические и гуманитарные аспекты информационной безопасности. Материалы III Всерос. научнопракт. конф. Пятигорск: ПГУ, 2022. – С. 24-27.