

БЕЗОПАСНОСТЬ И УДОБСТВО ИНТЕРНЕТ-САЙТОВ

A'zamjonova Zarinaxon To'xtasin qizi
Ma'rufjonov Maqsudjon Mansurjon o'g'li
Mamadaliyeva Barnoxon Ozodbek qizi

Студенты Ферганского филиала ТУИТ имени Мухаммеда аль-Хорезмий

Аннотация: *Веб-страницы используют протокол передачи гипертекста (HTTP) и механизмы безопасности шифрования (HTTP Secure). Роль веб-сайта в мире Интернета важна. Поэтому обеспечение безопасности веб-сайтов необходимо для предотвращения цифровых преступлений. Преступники нацелены на самые разные ситуации, о которых люди не знают. Безопасность имеет решающее значение для важных веб-сайтов, таких как банковские, правительственные, торговые и другие. Эффективная программа безопасности направлена на снижение риска посредством осведомленности, предотвращения, обнаружения и измерения. Не существует такой вещи, как идеальная безопасность, и решительного злоумышленника можно победить или почти обойти.*

Ключевые слова: *Безопасность, Шифрование, Онлайн-услуги, Обмен информацией, Вредоносное ПО и вирусы, Информация о пользователе, Взлом и кража личных данных, Фишинг.*

В современную цифровую эпоху веб-сайты - это средства связи, порталы, коммерция и информация. Это важно для предприятий и организаций, которые служат платформой для обмена стал компонентом. Однако доверие к сайтам растёт кроме того, ущерб важной информации на сайте, репутации владельцев сайта. киберугрозы, которые наносят ущерб и даже финансовые потери риск увеличивается. Для владельцев веб-сайтов сделать безопасность сайта приоритетом и сделать их принятие мер по защите от киберугроз, чем когда-либо преждеважнее. В статье рассматривается важность безопасности веб-сайтов, с которыми сталкиваются веб-сайты распространенные типы киберугроз и что они собой представляют теоретические и практические навыки по защите.

Безопасность веб-сайта — это меры и методы, используемые для защиты веб-сайта от несанкционированного доступа, кражи данных и других типов киберугроз.

Безопасность веб-сайта важна по нескольким причинам:



- Во-первых, веб-сайты часто хранят конфиденциальную информацию, например личную информацию или правительственную тайну, которая может стать желательной целью для киберпреступников.

- во-вторых, успешная кибератака на веб-сайт может привести к репутационному ущербу, финансовым потерям и юридической ответственности.

- В-третьих, веб-сайты часто являются частью ИТ-инфраструктуры бизнеса и взаимосвязаны, а это означает, что нарушение безопасности может распространиться на другие системы и устройства. В целом безопасность веб-сайта является важным аспектом обеспечения конфиденциальности, целостности и доступности данных и ресурсов веб-сайта.

Безопасность и удобство интернет-сайтов зависит от ряда ключевых факторов. Этими факторами могут быть:

Безопасность: Безопасность интернет-сайтов очень важна для пользователей сайта. Безопасность включает в себя обеспечение защиты персональных данных в процессе доступа к сайту и получения информации с сайта. Для этой цели используются протоколы безопасности, такие как сертификаты SSL и сквозное шифрование. **Легко найти и получить информацию:** Интернет-сайты позволяют пользователям находить и получать необходимую информацию. Через эти сайты можно искать, изучать и использовать любую имеющуюся информацию.

Шифрование: Личная информация пользователей должна быть защищена шифрованием данных, передаваемых через веб-сайты. Эти протоколы шифрования затрудняют доступ к данным пользователей для поддержки хакеров.

Использование протокола HTTPS: Установление зашифрованного соединения с вашим сайтом с использованием протокола HTTPS имеет важное значение для шифрования и безопасности данных. Установка сертификата SSL и использование протокола HTTPS дает пользователям уверенность в защите своих данных.

Онлайн-услуги. Через веб-сайты пользователи могут получать необходимые им услуги онлайн. Например, через интернет-магазины можно приобретать любые товары, управлять счетом через банки, создавать и отправлять электронные документы.

Обмен информацией: Интернет-сайты позволяют пользователям обмениваться информацией. Эти сайты позволяют вам читать новости,



писать и читать блоги, а также получать доступ к базам данных и использовать их.

Это всего лишь несколько примеров безопасности и удобства интернет-сайтов. Возможности Интернета для обмена интересами, информацией и общением очень широки и могут быть полезны каждому.

Проблемы с безопасностью веб-сайта могут быть вызваны следующими основными факторами:

1. Вредоносное ПО и вирусы. Вредоносное ПО и вирусы могут быть установлены на устройства пользователей через интернет-сайты. Когда пользователи загружают файлы, нажимают на рекламные баннеры или нажимают на подозрительные ссылки на этих сайтах, на устройства пользователя может быть установлено вредоносное ПО.

2. Информация о пользователе: Интернет-сайты могут собирать и хранить личную информацию пользователей. Эта информация включает в себя личную информацию, такую как имя пользователя, адрес электронной почты, номер телефона. Если на сайте не реализованы необходимые методы анализа и защиты для обеспечения безопасности, данные пользователя могут быть открыты для поддержки хакеров.

3. Взлом и кража личных данных. Интернет-сайты предоставляют возможность взлома учетных записей пользователей. Если системы безопасности сайта не работают, хакер сможет получить доступ к сайту и узнать личность пользователя.

4. Фишинг. Фишинговые атаки на пользователей возможны через Интернет-сайты. С помощью этих сканеров веб-сайты, похожие на сайт, пытаются собирать личную информацию пользователей. В этой форме логины, пароли и другая личная информация пользователей о банковских счетах могут быть доступны хакерской поддержке.

Для повышения уровня безопасности Интернет-сайтов можно реализовать следующие рекомендации:

Надежные пароли и аутентификация. Мы рекомендуем пользователям использовать надежные и безопасные пароли. Пароли должны содержать комбинацию длины, прописных и строчных букв, цифр и символов. Также неплохо использовать двухфакторную аутентификацию (например, коды SMS или проверку приложения для двухфакторной аутентификации).

Защита от DDoS-кошельков: DDoS-кошельки могут быть заблокированы на сайте и привести к прекращению работы сайта. В этом случае рекомендуется использовать такие методы, как установка DDoS-



защиты, защита от атак с использованием дополнительных серверов, ограничение источника IP и фильтрация трафика.

Эти рекомендации могут помочь улучшить безопасность сайта. Также важно проверить настройки безопасности сайта, чтобы обеспечить безопасность, и использовать многоуровневые стратегии защиты данных.

УДОБСТВО:

- **Интуитивный дизайн интерфейса:** Простой и интуитивный интерфейс, который позволяет пользователям легко ориентироваться и выполнять нужные действия.

- **Адаптивный дизайн:** Оптимизация сайта для работы на различных устройствах и разрешениях экранов, чтобы обеспечить удобство использования на компьютерах, планшетах и смартфонах.

- **Быстрая загрузка страниц:** Оптимизация ресурсов сайта, чтобы страницы загружались быстро, улучшая общий опыт пользователя.

- **Ясная навигация:** Легкость в поиске и перемещении по сайту с четкой и информативной навигацией.

- **Доступность:** Обеспечение доступности для пользователей с ограниченными возможностями, такими как поддержка сенсорных устройств, экранных читалок и других адаптивных технологий.

- **Минимизация количества шагов:** Упрощение процессов, чтобы пользователи могли легко достигнуть своих целей с минимальным количеством действий.

Обеспечение баланса между безопасностью и удобством является важным аспектом разработки и поддержки интернет-сайтов, поскольку оба аспекта сильно влияют на общее восприятие и удовлетворение пользователей.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

1. Umaraliyev, J., Abdurakhimov, O., & Isokjonova, S. (2023, June). USE AND EFFECTIVENESS OF INFORMATION TECHNOLOGIES IN MEDICINE. In Academic International Conference on Multi-Disciplinary Studies and Education (Vol. 1, No. 11, pp. 148-151).

2. Umaraliyev, J., Turdaliyev, K., Isoqjonova, S., & Abdurakhimov, O. (2023). ITS APPLICATIONS AND PROSPECTS IN EDUCATION. Interpretation and Researches, 1(11). search the horse



3. O Abduraximov, A Tojiddinov, U Nazirjonov. IDENTIFICATION AND AUTHENTICATION IN INFORMATION SECURITY. NETWORK DISPLAY TECHNOLOGY. Академические исследования в современной науке, 2023. (Vol. 2, No. 21, pp. 26-32).

4. AO Azimjon o'g'li, TA Ilhomjon o'g'li . NETWORK OPERATING SYSTEMS. XALQARO ANIQ FANLAR TAHLILI, 2023. (Vol. 1, No. 2, pp. 51-54).

5. AO Azimjon o'g'li, TA Ilhomjon o'g'li, NU Nozimjon o'g'li.

AVTOTRANSPORT VOSITALARINI KIBERHUUJUMLARDAN HIMOYA QILISH BO ‘YICHA YO ‘L XARITASI . Новости образования: исследование в XXI веке, 2023. (Vol. 2, No. 13, pp. 70-74).

6. TK Ilhomjon, AO Azimjon, NU Nazimjon. CLOUD TECHNOLOGIES AND CLOUD COMPUTING JOURNAL OF SCIENCE, RESEARCH AND TEACHING, 2023. (Vol. 2, No. 8, pp. 79-81).

7. TA Ilhomjon o'g'li, AO Azimjon o'g'li, ANDROID XAVFSIZLIGI, XAVFSIZLIK TIZIMLARINI YAXSHILASH. PEDAGOG, 2023. (Vol. 6, No. 6, pp. 753-757).

8. NU Nozimjon o'g'li, AO Azimjon o'g'li, TA Ilhomjon o'g'li. Information and Communication Technologies in Education LMS Systems. American Journal of Public Diplomacy and International Studies (2993-2157). (Vol. 1, No. 6, pp. 28-31).

9. AO Azimjon o'g'li, TA Ilhomjon o'g'li, NU Nozimjon o'g'li . Lms Systems and Their Description. American Journal of Public Diplomacy and International Studies (2993-2157). (Vol. 1, No. 6, pp. 22-24).

10. NU Nozimjon o'g'li, AO Azimjon o'g'li, TA Ilhomjon o'g'li. Education to Give in Processes Information and Communication Technologies. American Journal of Public Diplomacy and International Studies (2993-2157). (Vol. 1, No. 6, pp. 18-21).

11. TA Ilhomjon o'g'li, NU Nozimjon o'g'li, AO Azimjon o'g'li. Grid Analysis and Design. American Journal of Public Diplomacy and International Studies (2993-2157). (Vol. 1, No. 6, pp. 25-27).

12. NU Nozimjon o'g'li, AO Azimjon o'g'li, TA Ilhomjon o'g'li . Информационные И Коммуникационные Технологии В Образовании LMS Системы. American Journal of Science on Integration and Human Development (2993-2750). (Vol. 1, No. 6, pp. 17-20).

13. AO Azimjon o'g'li, TA Ilhomjon o'g'li, NU Nozimjon o'g'li. The Evolution of Graphical Interfaces for Programming TRACE MODE 6



Algorithms. American Journal of Pediatric Medicine and Health Sciences (2993-2149). (Vol. 1, No. 6, pp. 72-74).

14. TA Ilhomjon o'g'li, NU Nozimjon o'g'li, AO Azimjon o'g'li. Grid Tahlil Va Loyihalash. American Journal of Public Diplomacy and International Studies (2993-2157). (Vol. 1, No. 5, pp. 132-134).

15. NU Nozimjon o'g'li, AO Azimjon o'g'li, TA Ilhomjon o'g'li. Ta'lim Berish Jarayonlarida Axborot-Kommunikatsiya Texnologiyalari. American Journal of Language, Literacy and Learning in STEM Education (2993-2769). (Vol. 1, No. 6, pp. 26-29).

16. AO Azimjon o'g'li, TA Ilhomjon o'g'li, NU Nozimjon o'g'li. Lms Tizimlari Va Ularning Tavsifi. American Journal of Engineering, Mechanics and Architecture (2993-2637). (Vol. 1, No. 6, pp. 36-38).

17. U Jamshidbek To'xtasin o'g, AO Azimjon o'g'li. THE TRANSFORMATIVE ROLE AND IMPORTANCE OF TELECOMMUNICATION TECHNOLOGIES IN OUR DAILY LIVES " ONLINE-CONFERENCES" PLATFORM, 2023. (pp. 138-139).

18. K Turdaliyev, O Abduraximov, S Isoqjonova. OPPORTUNITIES OF DIGITAL TECHNOLOGIES. Наука и инновация, 2023. (Vol. 1, No. 15, pp. 8-11).

19. Isoqjonova, S., Abduraximov, O., & Turdaliyev, K. (2023). ZAMONAVIY DUNYODA ROBOTLARNING O'RNI HAMDA AHAMIYATI. Talqin Va Tadqiqotlar, 1(10).

20. Nafisaxon, T. U., Jamshidbek To'xtasin o'g, U., Arsenevna, D. E., & Azimjon o'g'li, A. O. (2022). AVTOMATLASHTIRILGAN AVTOTURARGOH IMKONIYATLARI VA QULAYLIKLARI. INNOVATION IN THE MODERN EDUCATION SYSTEM, 3(25), 45-48.

21. Tashlanova , N., & Abduraximov , O. (2023). TURIZM SOHASIDAGI ELEKTRON TIJORAT. Research and Implementation. извлечено от <https://fer-teach.uz/index.php/rai/article/view/809>

22. K Turdaliyev, O Abduraximov, J Umaraliyev. (2023). FOCL AFZALLIKLARI HAMDA KAMCHILIKLARI. MOBIL SU'NIY YO'LDOSH VA OPTIK TOLALI TARMOQLAR. Development of pedagogical technologies in modern sciences. 2(4), 123-128.

23. TK Ilhomjon o'g'li, AO Azimjon o'g'li, NH Maxmudjon o'g'li, (2022). MASOFAVIY TA'LIM MODELLARI VA MASOFADAN OQITISH TIZIMLARI. SUSTAINABILITY OF EDUCATION, SOCIO-ECONOMIC SCIENCE THEORY, 1(4), 113-116.



24. U Jamshidbek To'xtasin o'g, TA Ilhomjon o'g'li, AO Azimjon o'g'li, (2022). AXBOROTLARNI AVTOMATLASHTIRILGAN BOSHQARUV TIZIMI. PEDAGOGICAL SCIENCES AND TEACHING METHODS, 2(17), 22-25

25. Абдурахимов , О. А., & Махмудов , У. Р. (2023). ПРЕИМУЩЕСТВА И НЕДОСТАТКИ ВОЛОС, МОБИЛЬНЫХ СПУТНИКОВЫХ И ОПТИЧЕСКИХ СЕТЕЙ. Educational Research in Universal Sciences, 2(6), 147–150. Retrieved from <http://erus.uz/index.php/er/article/>

26. Umaraliyev , J. T. o'g'li, Isoqjonova , S. I. qizi, & Abduraximov , O. A. o'g'li. (2023). REVOLUTIONIZING INDUSTRIES AND SHAPING THE FUTURE. GOLDEN BRAIN, 1(17), 347–350

