Информационно-психологическая безопасность в открытых информационных системах

Азизабону Акбаровна Абдуллоева
a1abdullaeva09@gmail.com
Мехрангиз Уктамовна Ахророва
akhrorova2003@gmail.com
Ринат Фаритович Бурнашев
rinat.burnashev@inbox.ru
Самаркандский государственный институт иностранных языков

Аннотация: В статье рассматриваются основные угрозы для информационно-психологической безопасности, которые могут возникнуть при использовании открытых информационных систем. В частности, авторы описывают риски, связанные с распространением личной информации, манипуляцией мнениями, предоставлением непроверенной информации и т.д. Далее в статье представлены существующие меры для обеспечения информационно-психологической безопасности в открытых информационных системах.

Ключевые слова: фейковые новости, дезинформация, кибербуллинг, онлайн-жестокость, распространение непристойного контента, манипуляция мнениями и убеждениями, модерация контента, фильтрация информации

Information and psychological security in open information systems

Azizabonu Akbarovna Abdulloeva
a1abdullaeva09@gmail.com
Mehrangiz Uktamovna Akhrorova
akhrorova2003@gmail.com
Rinat Faritovich Burnashev
rinat.burnashev@inbox.ru
Samarkand State Institute of Foreign Languages

Abstract: The article discusses the main threats to information and psychological security that may arise when using open information systems. In particular, the authors describe the risks associated with the dissemination of personal information, manipulation of opinions, provision of unverified information, etc. Further, the article

presents existing measures to ensure information and psychological security in open information systems.

Keywords: fake news, disinformation, cyberbullying, online cruelty, distribution of obscene content, manipulation of opinions and beliefs, content moderation, information filtering

Проблема информационно-психологической безопасности в открытых информационных системах остается актуальной в связи с тем, что сегодня все больше людей используют интернет, социальные сети и другие открытые информационные системы. Это приводит к росту угроз, связанных с психологическим воздействием информации на пользователей.

Основные угрозы для информационно-психологической безопасности включают распространение фейковых новостей и дезинформации, кибербуллинг и онлайн-жестокость, распространение непристойного контента, манипуляцию мнениями и убеждениями, а также другие формы негативного воздействия.

Для защиты информационно-психологической безопасности в открытых информационных системах необходимо использовать комплекс мер, включающий технические и организационные меры. Корректная модерация контента, использование надежных и проверенных источников информации, обучение умению определять фейковую информацию и дезинформацию - все это может помочь защитить пользователей от негативных воздействий на их психологическое состояние.

Таким образом, проблема информационно-психологической безопасности в открытых информационных системах является актуальной и требует комплексного подхода к ее решению.

Тема информационно-психологической безопасности в открытых информационных системах является актуальной в современном мире. С ростом использования интернета и социальных сетей все больше пользователей становятся жертвами негативного воздействия информации на их психологическое состояние.

Распространение фейковых новостей и дезинформации, кибербуллинг и онлайн-жестокость, распространение непристойного контента, манипуляция мнениями и убеждениями - все эти угрозы могут привести к серьезным психологическим проблемам у пользователей, включая депрессию, тревожность, социальную напряженность и другие негативные состояния.

Кроме того, рост угроз информационно-психологической безопасности может привести к возникновению новых форм киберпреступности, что усугубляет ситуацию в области информационной безопасности.

Таким образом, проблема информационно-психологической безопасности в открытых информационных системах является актуальной и требует немедленных действий для ее решения. Комплексный подход к проблеме позволит защитить пользователей от негативного воздействия информации на их психологическое состояние и уменьшить уровень угроз в области информационной безопасности.

Распространение фейковых новостей и дезинформации является одной из основных угроз для информационно-психологической безопасности в открытых информационных системах. Фейковые новости или дезинформация - это намеренное искажение фактов или создание ложных сообщений с целью дезориентации и манипуляции мнениями аудитории.

Распространение фейковых новостей и дезинформации может привести к панике и социальной напряженности, а также осложнить принятие важных решений. Например, в политической сфере распространение дезинформации может повлиять на выборы и сделать общественное поле менее стабильным и предсказуемым. Кроме того, фейковые новости могут вызвать панику среди населения, что особенно опасно в ситуациях экстремальных ситуаций, например, при наводнениях, огромных пожарах и других катастрофах.

Для преодоления угрозы, связанной с распространением фейковых новостей и дезинформации, можно использовать несколько подходов. Во-первых, следует использовать проверенные источники информации и проверять другие источники на достоверность. Во-вторых, необходимо обучать пользователей умению определять фейковые новости и дезинформацию и находить надежные источники информации. В-третьих, важно проводить мониторинг дезинформации и оперативно реагировать на ее распространение.

Таким образом, распространение фейковых новостей и дезинформации является серьезной угрозой для информационно-психологической безопасности в открытых информационных системах. Решение этой проблемы требует комплексного подхода, включающего в себя технические, организационные и образовательные меры.

Кибербуллинг и онлайн-жестокость - это формы негативного воздействия на психологическое состояние пользователей в открытых информационных системах. Кибербуллинг - это форма электронного насилия, которая проявляется в постоянных оскорблении, унижениях, угрозах и других формах онлайн-жестокости.

Кибербуллинг может привести к серьезным психологическим травмам у пострадавших и оказать негативное воздействие на их психологическое состояние. Кроме того, онлайн-жестокость может вызвать чувство страха,

паранойи и дискомфорта у пользователей, что может привести к ухудшению самочувствия и увеличению уровня тревожности.

Для борьбы с кибербуллингом и онлайн-жестокостью необходимо принимать несколько мер. Во-первых, следует обучать пользователей безопасным практикам использования интернета. Важно объяснять, каким образом происходит кибербуллинг и как можно избежать его. Во-вторых, следует разрабатывать и внедрять политики компаний и социальных сетей, которые будут предупреждать и предотвращать акты онлайн-жестокости. В-третьих, важно обучать пользователей умению реагировать на кибербуллинг и онлайн-жестокость и сообщать о подобных случаях компетентным органам.

Таким образом, кибербуллинг и онлайн-жестокость представляют серьезную угрозу для информационно-психологической безопасности в открытых информационных системах. Решение этой проблемы требует обучения пользователей безопасным практикам использования интернета и разработки политик компаний и социальных сетей по предотвращению и борьбе с онлайн-жестокостью.

Распространение непристойного контента - еще одна угроза для информационно-психологической безопасности в открытых информационных системах. Непристойный контент может включать в себя изображения или тексты, которые содержат сексуальный характер, насилие или другие оскорбительные материалы, что может привести к негативному влиянию на психологическое состояние пострадавших, особенно детей и подростков.

Распространение непристойного контента может привести к панике, стрессу и дискомфорту у пользователей, которые вынуждены столкнуться с этим контентом. Кроме того, подобный контент может привести к увеличению уровня агрессии и насилия в обществе.

Манипуляция мнениями и убеждениями - это процесс воздействия на человека или группу людей с целью изменения их мнения, убеждений и поведения в соответствии с интересами и целями манипулятора. Этот процесс может быть осуществлен различными способами, такими как использование ложной информации, политической риторики, обмана, пропаганды, а также манипуляции эмоциями и страхами людей. Манипуляция мнениями и убеждениями может приводить к негативным последствиям, таким как ограничение свободы мысли и выражения, разрушение доверия в обществе, усиление стереотипов и предубеждений, а также ухудшение качества жизни людей.

Модерация контента - это одна из технических мер защиты информационно-психологической безопасности, которая заключается в контроле и управлении содержимым, например, на сайте, форуме, в социальных

сетях и т.д. Модерация контента осуществляется специально назначенными сотрудниками или модераторами, которые проверяют все размещаемые на площадке сообщения, комментарии, фото и видео на соответствие правилам и законам.

Модерация контента может включать в себя такие действия, как удаление сообщений, заблокирование пользователей, временное ограничение доступа к площадке, предупреждения и т.д.

Целью модерации контента является обеспечение безопасной и удобной среды для пользователей, обеспечение соблюдения правил и законов и защита от нежелательного или опасного контента, такого как насилие, ненависть, дискриминация, мошенничество и т.д.

Фильтрация информации - это одна из технических мер защиты информационно-психологической безопасности, которая заключается в управлении потоком данных с целью отсеивания нежелательных или опасных для пользователя информационных сигналов.

Фильтрация информации может осуществляться на различных уровнях, от сетевого до прикладного, и может включать в себя следующие меры:

- блокирование определенных сайтов, IP-адресов, доменов или URL-адресов, содержащих нежелательный или опасный контент;
- фильтрация электронной почты и блокирование спама, вредоносных файлов и phishing-атак;
- ограничение доступа к определенным приложениям, сервисам или ресурсам внутри организации с целью предотвращения утечки конфиденциальной информации;
- фильтрация поисковых запросов и блокирование результатов поиска, содержащих нежелательный контент;
- ограничение функциональности программ и сервисов для сохранения установленных пользователем ограничений.

Целью фильтрации информации является снижение риска получения пользователем нежелательного или опасного контента, защита от утечки конфиденциальной информации или защита компьютерной сети от вредоносных программ и других нежелательных воздействий.

Удаление угрожающего или оскорбительного контента - это одна из технических мер защиты информационно-психологической безопасности, которая заключается в удалении нежелательного контента из информационного пространства.

Удаление угрожающего или оскорбительного контента может осуществляться на различных площадках, включая социальные сети, онлайн-форумы, блоги и т.д. Модераторы и администраторы данных платформ следят за

контентом, который размещают пользователи, и при необходимости удаляют или блокируют нежелательный контент, нарушающий правила использования этих платформ или законодательные требования.

Целью удаления угрожающего или оскорбительного контента является защита пользователей от жестокого и угрожающего поведения других пользователей, а также обеспечение безопасной и комфортной среды для общения и обмена информацией в информационном пространстве.

Разработка и внедрение системы предупреждения и реагирования на нарушения информационно-психологической безопасности - это одна из организационных мер защиты информационно-психологической безопасности, которая заключается в создании процедурных и технических мер для обнаружения, анализа и устранения угроз информационной безопасности.

Система предупреждения и реагирования на нарушения информационно-психологической безопасности может включать в себя следующие меры:

- установление процедурных инструкций и регламентов по обеспечению информационной безопасности и реагированию на инциденты;
- проведение регулярных аудитов информационной безопасности с целью выявления уязвимостей и возможных угроз;
- обучение персонала мерам обеспечения информационной безопасности и процедурам реагирования на инциденты;
- создание систем мониторинга и анализа информации с целью обнаружения и предупреждения потенциальных угроз;
- разработка планов эвакуации, резервирования данных и восстановления после инцидентов.

Целью разработки и внедрения системы предупреждения и реагирования на нарушения информационно-психологической безопасности является повышение эффективности действий при атаке на информационные ресурсы, обеспечение быстрого и эффективного реагирования на инциденты и снижение риска потери конфиденциальной информации.

Обучение пользователей безопасным практикам использования открытых информационных систем - это одна из организационных мер защиты информационно-психологической безопасности, которая заключается в подготовке и обучении пользователей основам информационной безопасности и безопасным практикам на открытых информационных системах.

Неподготовленному человеку очень сложно распознать негативное информационное воздействие, если оно применяется, поэтому очень актуальными становятся вопросы связанные с техниками противостояния негативному информационному влиянию и вопросам образования в области информационной безопасности.

Способ защиты 1-й: «Уход» - увеличение дистанции, прерывание контакта, выход за пределы досягаемости информационного воздействия. Действия в различных информационных ситуациях могут быть такими: отключение определенных каналов СМИ (раздражающего канала телевидения, выход из Интернета и пр.), отказ от просмотра (прослушивания) конкретных теле-радиопрограмм; отказ от чтения некоторых газет, статей, рубрик и пр.; уход, под различными предлогами, с массовых зрелищных мероприятий: театра, концертного зала, кинотеатра и пр., митингов, собраний и др.; смена неприятной темы беседы, стремление не обострять межличностные отношения во время беседы (обход «скользких тем», «острых углов» и пр.), уклонение от встреч с теми, кто является источником неприятных переживаний, прерывание под различными предлогами встреч, бесед.

Способ защиты 2-й: «Блокировка» - контроль информационного воздействия, выставление психологических барьеров, ограждение психики от внешнего негативного информационного воздействия.

Способ защиты 3-й: «Затаивание» - контроль своей реакции на внешнее информационное воздействие. Выполняемые действия: отсрочка своих реакций, поспешных выводов и оценок, задержка или отказ от действий и поступков, вызываемых информационным воздействием; маскировка, сокрытие чувств, проявлений эмоций и др.

Обучение пользователей безопасным практикам использования открытых информационных систем может включать в себя следующие меры:

- проведение тренингов и семинаров по информационной безопасности, участие в которых обязательно для всех сотрудников организации;
- разработка методических материалов и инструкций по безопасному использованию информационных технологий и открытых информационных систем;
- оформление графических плакатов и брошюр для распространения информации о методах и способах взлома и атаки на ИТ-системы в наглядной форме;
- обязательное использование двухфакторной аутентификации и сложных паролей для доступа к системам с конфиденциальной информацией;
- повышение осведомленности пользователей об угрозах безопасности в социальных сетях и спам-рассылках, а также о методах их обнаружения и защиты;
- регулярное обновление программного обеспечения и антивирусных программ на компьютерах пользователей, а также принятие мер по ограничению доступа к системам с конфиденциальной информацией.

Целью обучения безопасным практикам использования открытых информационных систем является повышение осведомленности и знаний сотрудников об угрозах информационной безопасности, формирование у них навыков и привычек безопасного поведения в Интернете, а также снижение риска потери конфиденциальной информации или денежных средств.

Использование надежных и проверенных источников информации - это одна из практических рекомендаций по обеспечению информационно-психологической безопасности в открытых информационных системах.

При использовании открытых информационных систем пользователи должны помнить, что многие ресурсы могут содержать ложную и недостоверную информацию, а также могут быть источником угроз безопасности (вирусы, мошеннические сайты и т.д.).

Для обеспечения безопасности при использовании открытых информационных систем рекомендуется следующее:

- проверяйте надежность источников информации, особенно если речь идет о финансовых или личных данных;
- используйте только официальные и проверенные сайты организаций и государственных институтов;
- избегайте подозрительных сайтов и ссылок, которые могут содержать вирусы или посредничать в краже личных данных;
- следите за сроком действия антивирусных программ, обновляйте их регулярно и проверяйте компьютер на наличие вирусов;
- отключайте автоматические загрузки приложений или дополнений при посещении сайтов;
- следите за настройками конфиденциальности на социальных сетях и других интернет-ресурсах, и не сообщайте свои личные данные (реквизиты, пароли и т.д.) неизвестным пользователям.

Целью использования надежных и проверенных источников информации является снижение риска получения ложной или недостоверной информации, а также защита от угроз безопасности при использовании открытых информационных систем.

Обучение умению определять фейковую информацию и дезинформацию - еще одна практическая рекомендация по обеспечению информационно-психологической безопасности в открытых информационных системах.

В Интернете существует множество фейковых новостей, статей и другой информации, которая может быть использована для манипуляции мнением, распространения нежелательной информации и других преступных действий. Пользователи открытых информационных систем должны научиться различать

фейковую информацию и дезинформацию для того, чтобы защитить свои интересы.

Политики компаний по обеспечению безопасности пользователей:

1. Сохранять конфиденциальность данных пользователей. Это означает, что все личные данные пользователей, такие как пароли, имена, адреса электронной почты, необходимо хранить в зашифрованном виде.

2. Использовать сильные пароли. Пользователи должны обязательно использовать длинные пароли из букв, цифр, знаков препинания и специальных символов. Особенно важно, чтобы пароли не были связаны с личными данными пользователя, такими как имена или даты рождения.

3. Установить мощную систему аутентификации. В дополнение к паролю, можно использовать двухэтапную проверку, чтобы убедиться в личности пользователя.

4. Сохранять данные на безопасных серверах. Серверы должны быть размещены в безопасных помещениях, защищенных от несанкционированного доступа.

5. Установить мощную защиту от вирусов и атак. Необходимо использовать софтверные решения, которые могут обнаружить и предотвратить атаки на систему.

6. Информировать пользователей о возможных угрозах. Компании должны предоставлять информацию о возможных угрозах безопасности, таких как фишинг, мошенничество и вредоносный код.

7. Организовать тренинги и обучение для пользователям. Компании должны проводить тренинги и обучение для пользователей, чтобы обучить их, как избегать угроз безопасности в Интернете.

8. Проводить регулярный мониторинг безопасности. Компании должны регулярно проверять безопасность своих систем и устанавливать любые необходимые обновления и патчи.

9. Обеспечивать быстрый отклик на инциденты безопасности. Если происходит инцидент безопасности, компания должна быстро реагировать и принимать необходимые меры для защиты пользователей.

10. Сотрудничать с правоохранительными органами. Если компания обнаруживает преступную деятельность, она должна незамедлительно сообщать об этом правоохранительным органам.

Проблема информационно-психологической безопасности в открытых информационных системах является актуальной и важной для пользователей и компаний. Каждый день мы сталкиваемся с новыми угрозами безопасности, которые могут привести к утечке личной информации, гибели денег и даже причинить вред нашему здоровью.

Для обеспечения безопасности в открытых информационных системах необходимо применять комплексный подход, который включает использование сильных паролей, мощных систем аутентификации и защиты от вирусов и атак, проведение тренингов и обучения пользователей, регулярный мониторинг безопасности и быстрый отклик на инциденты безопасности.

Каждая компания должна выработать свою политику по обеспечению безопасности пользователей и работать с правоохранительными органами, если обнаруживаются преступные действия. Безопасность в открытых информационных системах должна быть на высоком уровне, чтобы пользователи могли максимально защитить свои личные данные и избежать угроз со стороны внешних лиц.

Несмотря на уже достигнутый прогресс в обеспечении информационно-психологической безопасности в открытых информационных системах, в данной области существует много проблем, угроз и вызовов, которые требуют дальнейших исследований и разработок. Некоторые из них включают:

1. Развитие новых методов злоупотребления информацией для ведения кибер-атак: захват устройств, информационный шпионаж, фишинг-атаки и мошенничество.

2. Создание новых методов и практик защиты данных, так как существующие системы защиты могут быть изобретены и взломаны хакерами.

3. Анализ социальных, психологических и культурных аспектов влияния открытых информационных систем на людей и общество.

4. Разработка более эффективных методов обучения пользователей, нацеленных на уменьшение риска утечки данных и повышение личной бережливости в Интернете.

5. Создание новых методов интеграции научных и технических ресурсов для достижения большей эффективности и стабильности систем обеспечения информационно-психологической безопасности.

6. Разработка новых алгоритмов и программных обеспечений для выявления и предотвращения кибер-атак изнутри и снаружи организации.

7. Исследование и исполнение законодательных и нормативных требований, которые обеспечивают поддержание защиты и соблюдения личных данных и прав пользователей в Интернете.

Дальнейшие исследования и разработки в этих областях обязательны для защиты открытых информационных систем от угроз безопасности и обеспечения безопасной работы пользователей и организаций в Интернете.

Использованная литература

1. Бурнашев Р.Ф., Бурнашева Ф.С., Норжигитова Ш.А. Нейролингвистическое программирование как инструмент информационно-психологического манипулирования // ЕВРОПА, НАУКА И МЫ: сборник научных публикаций международной научно-практической конференции.- Издательство «Education and Science» Чехия, Прага. - 2020. - С. 85-87.

2. Джуракулова С. Ш. и др. Методы мониторинга активности пользователя в сети Интернет в целях обеспечения безопасности в киберпространстве //Science and Education. - 2022. - Т. 3. - №. 7. - С. 76-85.

3. Бурнашев Р. Ф., Бурнашева Ф. С., Тамаева Д. Р. Роль новых информационных технологий в преобразовании социума на пороге информационного общества //Science and Education. - 2020. - Т. 1. - №. 3. - С. 250-254.

4. Бурнашев Р. Ф., Бурнашева Ф. С., Абдувохидова Ш. А. Становление и развитие теоретической инноватики на современном этапе //Science and Education. - 2020. - Т. 1. - №. 2. - С. 173-178.

5. Бурнашев Р. Ф., Бурнашева Ф. С. Разработка модели инновационного развития информационно-образовательной среды высшего учебного заведения //Технологическое образование и устойчивое развитие региона. - 2012. - Т. 1. - №. 1-1. - С. 80-87.

6. Бурнашев Р.Ф., Инкачилова А.М., Нематуллаева Н.Б. Роль цифровизации образовательного процесса в формировании цифровой образовательной среды. // Сборник научных трудов по материалам XXXVIII Международной научно-практической конференции «Наука. Образование. Инновации» (Россия, Анапа, 12 января 2022 г.). - Анапа: Изд-во «НИЦ ЭСП» в ЮФО, 2022. ISBN 978-5-95283-768-3. - С. 115-121.

7. Бурнашева Ф. С. и др. Психологические особенности общения в открытых информационных системах //Science and Education. - 2020. - Т. 1. - №. 2. - С. 364-367.

8. Бурнашев Р. Ф. и др. Информационно-коммуникационные технологии как фактор повышения эффективности организации обучения специальным дисциплинам //Непрерывное образование в современном мире: история, проблемы, перспективы. - 2016. - С. 236-239.

9. Бурнашева Ф. С., Бурнашев Р. Ф., Аллаёрова Н. А. Внедрение модульной объектно-ориентированной динамической обучающей среды для организации самостоятельной работы студентов вузов //Образование. Технология. Сервис. - 2015. - Т. 1. - №. 1. - С. 57-62.

10. Бурнашев Р. Ф., Джуракулова С. Ш., Рустамова З. Р. Технология процесса обучения как процедура совместной деятельности преподавателя и студента //Science and Education. - 2022. - Т. 3. - №. 2. - С. 1384-1391.

11. Бурнашев Р. Ф., Бурнашева Ф. С., Арипова Ф. З. Информатика как предметная область инновационной деятельности в организации учебного процесса в современных условиях //Инновационное развитие науки и образования: сборник научных публикаций международной научно-практической конференции (Казахстан, Павлодар. - 2020. - С. 255-257.

12. Бурнашев Р. Ф., Нематуллаева Н. Б. Особенности информационных образовательных технологий XXI века //Science and Education. - 2021. - Т. 2. - №. 3.

13. Бурнашев Р.Ф., Абдусамадова Ш.Ш. Особенности организации инклюзивного образования. // Сборник научных трудов по материалам XXX Международной научно-практической конференции «Современное состояние и перспективы развития науки и образования» (Россия, Анапа, 07 января 2022 г.). - Анапа: Изд-во «НИЦ ЭСП» в ЮФО, 2022. ISBN 978-5-95283-765-2. - С. 56-61.

14. Меликова М. Н. К вопросу взаимозависимости культуры и образования // Интернаука. - 2017. - №. 11-1. - С. 96-97.

15. Рустамова Д. Р., Саматова Н. Т., Бурнашев Р. Ф. Классификация современных электронных средств информации //Science and Education. - 2022. - Т. 3. - №. 12. - С. 434-449.

16. Бурнашев Р. Ф., Бурнашева Ф. С., Арипова Ф. З. Информатика как предметная область инновационной деятельности в организации учебного процесса в современных условиях //Инновационное развитие науки и образования: сборник научных публикаций международной научно-практической конференции (Казахстан, Павлодар.-2020.-С. 255-257. - 2020.

17. Бурнашев Р. Ф., Бурнашева Ф. С. Использование электронных образовательных ресурсов в самостоятельной работе студентов //Образование. Технология. Сервис. - 2014. - Т. 1. - №. 1. - С. 113-117.

18. Мардиева Р. А. и др. Обучение иностранным языкам с помощью IT технологий //Science and Education. - 2022. - Т. 3. - №. 6. - С. 1173-1180.

19. Бурнашева Ф. С., Бурнашев Р. Ф., Аллаёрова Н. А. Внедрение модульной объектно-ориентированной динамической обучающей среды для организации самостоятельной работы студентов вузов //Образование. Технология. Сервис. - 2015. - Т. 1. - №. 1. - С. 57-62.

20. Бурнашев Р. Ф. и др. Применение современных систем управления контентом (CMS) в системе высшего образования при переходе на модульную систему обучения //Образование. Технология. Сервис. - 2015. - Т. 1. - №. 1. - С. 51-57.