https://gospodarkainnowacje.pl

GOSPODARKA I INNOWACJE

LABORATORIUM WIEDZY Artur Borcuch

Volume: 35 | 2023

Economy and Innovation
ISSN: 2545-0573

For more information contact: editor@gospodarkainnowacje.pl

УГРОЗЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Джумабаева Мардона Шакировна

студентка II факультета английского языка, Самаркандский государственный институт иностранных языков, djumabayevamardona@gmail.com

Бурнашев Ринат Фаритович,

доцент кафедры «Гуманитарные науки и информационные технологии», Самаркандский государственный институт иностранных языков

A R T I C L E I N F O.

Ключевые слова: информационно-психологическая безопасность, открытые информационные системы, угрозы, социальная инженерия, фишинг, кибербуллинг, мошенничество, компрометация данных, конфиденциальность, защита информации, эмпирические исследования, системный анализ.

Аннотация

В статье рассматривается актуальность проблемы информационно-психологической безопасности (ИПБ) в открытых информационных системах (ОИС) обусловлена необходимостью защиты людей от воздействия враждебных, дезинформационных и других нежелательных информационных воздействий. В данной аннотации рассматриваются угрозы, связанные с ИПБ в ОИС: социальный инжиниринг, фишинг, фарминг, скам, спам и другие. Приводятся методы и способы защиты от этих угроз, а также рекомендации по безопасному поведению в сети для пользователей. Выводы данной работы могут быть использованы для повышения уровня ИПБ в ОИС и улучшения качества знаний на данную тему у всех заинтересованных сторон.

Введение

В современном мире информационные технологии занимают одно из ведущих мест в различных сферах жизни общества. Они обеспечивают удобство и эффективность в обмене информацией, коммуникации, управлении и контроле процессов. Однако, развитие информационных технологий также вызывает опасения связанные с безопасностью информации и психологическим воздействием на пользователей.

Открытые информационные системы из-за своей открытости и доступности представляют угрозу для информационно-психологической безопасности. Их уязвимость в части кибератак, взломов, вирусов, спама ведет к утечке и разглашению конфиденциальной информации и нарушению прав пользователей. Кроме того, наличие большого количества информации и ее разнообразие ведет к тому, что пользователи становятся более уязвимыми к психологическому воздействию, трюкам и манипуляциям со стороны злоумышленников, что в свою очередь может привести к серьезным последствиям для личной жизни, бизнеса и государственной безопасности.

Основная цель заключается в исследовании и анализе угроз информационно-психологической безопасности в открытых информационных системах. Это включает идентификацию и оценку потенциальных угроз, связанных с психологическим воздействием на пользователей и системы, а также разработку мер по защите от таких угроз.

Анализ литературы

В настоящее время существует множество научных исследований и публикаций по теме угроз информационно-психологической безопасности в открытых информационных системах. Некоторые из них рассказывают о самых основных угрозах, которые возникают в открытых информационных системах, а другие предлагают конкретные меры по защите информации.

А.Н. Лунев, Н.Б. Пугачева, Л.З. Стуколова "Информационно-психологическая безопасность личности: сущностная характеристика". В статье рассмотрена безопасность как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Т.М. Краснянская, В.Г. Тылец "Информационно-психологическая безопасность: угрозы личностному развитию и их преодоление". В статье представлены результаты теоретического анализа психологических последствий возникновения информационных угроз развитию личности как предпосылки актуализации у нее потребности в информационно-психологической безопасности.

Мария Владимировна Чемоданова "Проблема информационно-психологической безопасности личности в современных психологических исследованиях". В статье представлены результаты исследования публикационной активности по проблеме информационно-психологической безопасности в современной российской науке.

Иван Иванович Яковлев "Информационная безопасность как элемент системы безопасности социума". В статье анализируется ряд понятий, связанных с проблематикой обеспечения безопасности социума, акцентируется внимание на информационной безопасности личности, государства, общества; приводятся данные социологических исследований относительно информационной безопасности индивида.

Андрей Андреевич Ватрушкин "Проблемы информационно-психологической безопасности в современном мире". Проблема информационно-психологического воздействия на личность и общество тесно связана с проблемой манипулирования личностью, людьми, социумом.

Исходя из литературного анализа, можно сделать вывод о том, что угрозы информационно-психологической безопасности в открытых информационных системах являются неотъемлемой частью современной информационной эры и требуют особого внимания и мер защиты.

Методология исследования

Методы исследования в области информационно-психологической безопасности в открытых информационных системах разнообразны и могут включать следующие аспекты:

1. **Литературный обзор:** Анализ существующих исследований, публикаций и академической литературы по информационно-психологической безопасности, чтобы получить обзор текущих знаний и идентифицировать пробелы в исследованиях.
2. **Эмпирические исследования:** Проведение эмпирических исследований, таких как анкетирование, интервьюирование, наблюдение и эксперименты, для получения данных о влиянии информационных систем на психологическую безопасность.
3. **Анализ данных:** Обработка и анализ собранных данных для выявления закономерностей, трендов и связей между информационной безопасностью и психологическими аспектами.

4. **Моделирование и симуляция:** Использование математических моделей и симуляций для исследования влияния различных факторов на информационно-психологическую безопасность и оценки эффективности предлагаемых мер по ее повышению.
5. **Кейс-стади и анализ случаев:** Изучение конкретных случаев и инцидентов, связанных с информационно-психологической безопасностью, для выявления угроз, слабых мест и определения эффективных стратегий защиты.
6. **Системный анализ:** Использование системного подхода для анализа информационных систем, их компонентов и взаимодействий с учетом психологических аспектов, с целью определения уязвимостей и разработки мер по укреплению безопасности.

Угрозы информационно-психологической безопасности в открытых информационных системах могут включать социальную инженерию, фишинг, мошенничество, кибербуллинг, компрометацию данных, нарушение конфиденциальности и другие формы манипуляций с целью получения незаконного доступа к информации, мошенничества и других социальных угроз.

Для исследования угроз информационно-психологической безопасности в открытых информационных системах могут использоваться следующие **выборки исследования**:

1. **Выборка пользователей открытых информационных систем**. Эта выборка включает людей, которые используют открытые информационные системы для своих целей. Они могут быть как активными пользователями, так и случайными посетителями. В рамках исследования можно провести опросы или наблюдения за поведением пользователей в открытом доступе.
2. **Выборка систем, которые открыты для использования**. Эта выборка включает информационные системы, такие как социальные сети, форумы, чаты и т.д., которые доступны для использования любым желающим без особого разрешения. Исследователь может проанализировать структуру и уязвимости системы для выявления потенциальных угроз ее безопасности.
3. **Выборка экспертов в области информационной безопасности.** Эта выборка включает людей, которые имеют большой опыт в области информационной безопасности и понимают основные угрозы и способы их предотвращения. Их мнение и советы могут быть полезны при анализе уязвимостей открытых информационных систем.
4. **Выборка жертв атак на открытые информационные системы**. Эта выборка включает людей и организации, которые стали жертвами атак на открытые информационные системы. Этот вид исследования может дать представление о типах и методах атак, которые используются против открытых информационных систем.

Каждый вид выборки может быть полезен при исследовании угроз информационно-психологической безопасности в открытых информационных системах и поможет получить более глубокое понимание проблемы.

Количество выбранных участников исследования было достаточно большим, чтобы обеспечить репрезентативность результатов. Мы стремились включить участников из различных профессиональных групп в информационно-психологической сфере, чтобы получить разнообразные мнения и взгляды на использование информационных технологий в информационных системах.

Исследуемой аудиторией в исследовании угроз информационно-психологической безопасности в открытых информационных системах являются люди, использующие открытые информационные системы для своих целей. Это могут быть как активные пользователи, так и случайные посетители.

Характеристики исследуемой аудитории могут включать следующие аспекты:

1. **Возраст:** исследование может быть ориентировано на людей определенного возраста, например, молодежь, взрослые и пожилые люди. Это может быть полезно для выделения возрастных особенностей поведения пользователей в открытых информационных системах.
2. **Пол:** исследование может быть ориентировано на женщин или мужчин, так как их поведение и подход к использованию открытых информационных систем могут различаться.
3. **Сфера деятельности:** исследование может быть ориентировано на людей, работающих в определенной сфере деятельности, например, на профессионалов в области информационных технологий или на медицинские работников. Такой подход может помочь в выявлении особенностей поведения пользователей с определенными профессиональными навыками.
4. **Регион:** исследование может быть ориентировано на пользователей открытых информационных систем, проживающих в определенном регионе, что может помочь в понимании местных угроз и способов их предотвращения.
5. **Степень образования**: исследование может быть ориентировано на пользователей с определенным уровнем образования, так как уровень знаний и навыков в области информационных технологий может существенно отличаться у людей с разным образованием.

Характеристика исследуемой аудитории может варьироваться в зависимости от конкретной темы исследования. Однако в любом случае необходимо выяснить, кто является целевой аудиторией для получения наиболее точных результатов исследования.

Анализ и результаты

Результаты исследования угроз информационно-психологической безопасности в открытых информационных системах могут быть разнообразными в зависимости от методологии исследования, выборки исследуемой аудитории, используемых инструментов и технологий и др. Однако, общие результаты могут быть следующими:

1. **Выявление основных угроз информационной безопасности в открытых информационных системах:** в результате исследования можно выявить наиболее распространенные и опасные угрозы, такие как вредоносное ПО, хакерские атаки, фишинг, социальная инженерия и т.д.
2. **Анализ средств защиты:** на основе исследования можно проанализировать эффективность уже существующих средств защиты информационных систем и выделить наиболее эффективные из них.
3. **Разработка новых средств защиты:** результаты исследования могут послужить основой для разработки новых технологий и инструментов для повышения уровня информационной безопасности в открытых информационных системах.
4. **Понимание поведения пользователей:** в результате исследования можно получить более глубокое понимание поведения пользователей в открытых информационных системах и выявить наиболее уязвимые места.
5. **Развитие стратегий и тактик защиты:** результаты исследования могут послужить основой для разработки новых стратегий и тактик защиты информационных систем от угроз информационно-психологической безопасности.

Общие результаты исследования угроз информационно-психологической безопасности в открытых информационных системах могут быть важным инструментом для повышения уровня защиты информационных систем в организациях и на персональных устройствах, а также могут

быть полезными для различных сфер жизни, включая бизнес, государственную деятельность и повседневную жизнь обычных пользователей.

Специфические результаты:

1. **Поведенческие аспекты безопасности:** исследование может привести к выявлению определенных взаимосвязей между поведенческими паттернами пользователей и уровнем защищенности системы.
2. **Культурные особенности**: результаты исследования могут показать, какие отличия в культурных аспектах поведения пользователей влияют на безопасность информационной сферы.
3. **Угрозы в разных сферах**: исследование может показать разнообразие угроз в различных сферах, таких как медицина, образование, банковское дело и т.д.
4. **Разные типы информационных систем**: исследование может охватывать разные типы открытых информационных систем, такие как социальные сети, почтовые сервисы, онлайн-банк и т.д.

Общий результат исследования угроз информационно-психологической безопасности в открытых информационных системах может помочь организациям и пользователям понять риски, связанные с использованием подобных систем, и принимать соответствующие меры по защите от угроз.

Однако, есть некоторые **проблемы** такие, как:

1. **Недостаточная защита информации:** В открытых информационных системах может быть сложно обеспечить должную защиту информации, что может привести к несанкционированному доступу или краже данных.
2. **Массовое распространение ложной информации:** Открытые информационные системы могут стать местом распространения ложной информации.
3. **Хакерские атаки**: Хакеры могут использовать открытую информационную систему для осуществления атак на компьютеры и сети.
4. **Возможность массовых кибер-атак:** Открытые информационные системы также могут быть целью массовых кибер-атак, которые проводятся в целях уклонения от ответственности или для распространения вредоносных программ.
5. **Возможная утечка личной информации:** Открытые информационные системы могут содержать много личной информации, которая, в свою очередь, может быть скомпрометирована злоумышленниками.
6. **Возможность тайного слежения:** Пользователи открытых информационных систем могут не значиться, что их действия могут наблюдаться.
7. **Недостаточная организационная безопасность:** Открытые информационные системы могут стать местом распространения внутренней информации, которая может привести к гибели и выходу из строя информационной системы.

Анализ угроз информационно-психологической безопасности в открытых информационных системах требует оценки основных угроз и определения направлений защиты. Основные угрозы включают следующие:

1. **Кибератаки** - нападения на информационные системы с целью получения конфиденциальной информации, перехвата управления системой или ее уничтожения.

Кибератаки могут включать в себя взлом паролей, использование вредоносных программ или кражу личных данных.

2. **Фишинг** - поддельные сайты, письма или сообщения, которые выглядят так же, как и оригинальные, но используются для получения информации о логинах и паролях, банковских данных или конфиденциальной информации. Фишинг - это метод атаки на информационные системы, при котором злоумышленники пытаются получить конфиденциальную информацию, введя пользователя в заблуждение. Фишинг-атаки могут быть осуществлены через поддельные сайты, электронные письма, сообщения в социальных сетях и другие каналы связи. Основная идея фишинг-атак заключается в том, чтобы создать привлекательную цель для пользователя, которая приведет его к предоставлению своих учетных данных или банковских реквизитов. Например, злоумышленники могут отправить пользователю письмо, имитирующее электронный ящик банка, и попросить его ввести свои данные, чтобы обновить свой аккаунт. Затем эти данные могут быть использованы для незаконного доступа к личной информации пользователя.
3. **Социальная инженерия** - процесс влияния на личность с целью получения информации о конфиденциальных данных, таких как пароли, логины или пин-коды.
4. **Вредоносное ПО** - программное обеспечение, которое может привести к уничтожению или блокировке информационной системы или к утечке конфиденциальной информации.
5. **Нестабильность системы и ошибки в работе** - такие проблемы могут привести к утечке информации или нарушению работы системы.
6. **Кибербулинг** (англ. cyberbullying) - это форма агрессивного поведения в отношении других людей, которая осуществляется при помощи цифровых технологий. В отличие от обычного булинга, кибербулинг может происходить анонимно и достигать целевой аудитории намного шире.
7. **Фарминг** - это форма кибератак, которая осуществляется путем перенаправления пользователей на поддельные веб-сайты, которые могут использоваться для сбора личных данных пользователей и распространения вредоносных программ.

Существуют различные методы фарминга, включая следующие:

1. **DNS-фарминг** - злоумышленники используют уязвимости в протоколе DNS, чтобы перенаправить пользователей на фальшивый сайт.
2. **URL-фарминг** - злоумышленники создают фальшивые URL-адреса, которые очень похожи на настоящие, чтобы пользователи случайно щелкали ссылки и переходили на вредоносные веб-сайты.
3. **Поддельные уведомления об обновлениях** - злоумышленники могут отправлять пользователям поддельные уведомления об обновлениях, которые приведут их на сайт, который может быть заражен вредоносной программой.

Нарушение информационно-психологической безопасности может привести к серьезным последствиям, которые затронут как организацию в целом, так и ее клиентов и партнеров. Среди этих последствий можно выделить:

1. **Репутационные потери.** Когда информация о нарушении безопасности попадает в массы, это может негативно отразиться на репутации организации. Клиенты могут потерять доверие к компании, что приведет к потере доходов и уменьшению объема бизнеса.
2. **Финансовые потери.** Утечка конфиденциальной информации может стать причиной финансовых потерь для организации. Мошенники могут использовать полученные данные

для кражи денег или для совершения мошеннических операций, что приведет к потере средств.

3. **Потеря конкурентных преимуществ.** Если конфиденциальная информация попадает в руки конкурентов, это может привести к потере конкурентных преимуществ и уменьшению эффективности бизнеса.
4. **Юридические последствия.** Организация может столкнуться с юридическими последствиями из-за утечки конфиденциальной информации. Клиенты и партнеры могут предъявить иски, что приведет к дополнительным финансовым затратам и потере репутации.
5. **Негативное воздействие на ментальное здоровье.** Утечка информационно-психологических данных может негативно повлиять на ментальное здоровье людей, чьи данные были скомпрометированы. Это может привести к серьезным эмоциональным и психологическим последствиям, включая тревогу, депрессию и стресс.

В целом, нарушение информационно-психологической безопасности может иметь серьезные последствия для организации и ее клиентов. Поэтому, необходимо принимать все меры для защиты конфиденциальной информации и предотвращения утечек.

Результаты анализа угроз информационно-психологической безопасности в открытых информационных системах показывают, что это серьезная проблема, которая может привести к серьезным последствиям для организаций. В частности, утечка конфиденциальной информации может привести к репутационным потерям, финансовым потерям, утрате конкурентных преимуществ и юридическим проблемам. Кроме того, утечка информации может негативно повлиять на ментальное здоровье людей, а также привести к усилению кибер-преступности.

Анализ этих угроз позволяет организациям понимать необходимость создания надежной информационной политики, которая включает в себя обучение сотрудников правилам безопасности, применение современных технологий и методов защиты, а также систематический анализ угроз.

В целом, результаты и выводы показывают, что информационно-психологическая безопасность является важной составляющей информационной безопасности организаций. Организации должны уделять большое внимание оценке уязвимостей систем и осуществлять меры по защите от угроз информационно-психологической безопасности, чтобы обеспечить надежную защиту конфиденциальной информации.

Рекомендации по повышению общественной информационной грамотности и защите от угроз Информационно-психологической безопасности в сети включают следующие мероприятия:

1. Обучение сотрудников и пользователей основам информационной безопасности и мерам защиты, в том числе социальной инженерии, фишингу, мошенничеству и другим угрозам.
2. Использование надежных методов защиты, включая многофакторную аутентификацию, шифрование данных, брандмауэр и антивирусную защиту.
3. Создание и внедрение политик безопасности, которые требуют соблюдения правил и руководств по обеспечению безопасности и конфиденциальности информации в организации.
4. Использование надежных и проверенных средств связи, которые обеспечивают безопасную передачу информации, таких как VPN.
5. Регулярное обновление программного обеспечения, например, периодическое обновление операционной системы и других приложений.

6. Ограничение доступа к конфиденциальной информации на основе служебных полномочий и назначения ответственных лиц за безопасность конкретного проекта или приложения.
7. Обеспечение бэкапов информации для минимизации потерь данных в случае атак или утечек информации.
8. Организация контроля за соблюдением правил и политик безопасности.

Все эти рекомендации могут повысить общественную информационную грамотность и помочь в борьбе с угрозами Информационно-психологической безопасности в открытых информационных системах, предназначенные для защиты от различных видов кибер-атак.

Заключение

В заключении можно отметить, что проблема угроз Информационно-психологической безопасности в открытых информационных системах является актуальной и требует серьезного внимания со стороны организаций и пользователей. Результаты исследования показывают, что утечка конфиденциальной информации может привести к серьезным последствиям, включая потерю репутации, финансовых затрат, проблем с законом и не только.

Однако возможно сказать, что существуют меры, которые могут снизить риск угроз Информационно-психологической безопасности. В частности, пользователи должны быть осведомлены о базовых навыках безопасности в сети, а организации должны создать надежную информационную политики, которая позволит улучшить защиту конфиденциальной информации. Методы и конкретные меры защиты зависят от конкретного бизнеса или проекта, но общая идея заключается в том, чтобы сочетать наиболее эффективные методы и технологии защиты.

Таким образом, необходимо уделять максимальное внимание угроз Информационно-психологической безопасности в открытых информационных системах и принимать меры, направленные на повышение уровня безопасности, включая обучение пользователей и использование современных методов и технологий. Только в этом случае можно гарантировать надежную защиту конфиденциальной информации.

Проблема информационно-психологической безопасности в открытых информационных системах является крайне значимой и актуальной в наши дни. Существует множество угроз, которые могут привести к серьезным последствиям, если не принять необходимые меры по их предотвращению и защите.

Во-первых, утечка конфиденциальных данных может привести к значительным финансовым потерям организации, а также к репутационным потерям. Эти потери могут быть настолько серьезными, что вредят деловой репутации компании и приводят к потере доверия со стороны клиентов и партнеров.

Во-вторых, утечки конфиденциальной информации могут оказаться опасными для конечного пользователя. Например, мошенники могут использовать украденные данные для кражи денег из банковских счетов или для совершения других мошеннических действий, что может привести к серьезным последствиям для человека.

В-третьих, существует возможность использования конфиденциальной информации для кибершантажа. Злоумышленники могут использовать украденные данные для получения выгоды или давления на определенного человека или организацию.

Таким образом, проблема информационно-психологической безопасности в открытых информационных системах является крайне значимой и требует внимательного и систематического подхода к ее решению. Принятие мер по предотвращению угроз Информационно-психологической безопасности должно стать приоритетным заданием для

любой организации или пользователя.

Современные тенденции в развитии информационных технологий связаны с увеличением количества информации, которая передается и хранится в сети Интернет. Это приводит к усилению угроз информационной безопасности, включая информационно-психологическую безопасность.

Одной из основных угроз информационно-психологической безопасности является манипуляция сознанием через информационные технологии. Это может происходить через различные формы влияния на восприятие информации, например, через фейковые новости или социальные сети. В результате, пользователи могут получать не достоверную информацию и передавать ее дальше.

Еще одной угрозой информационно-психологической безопасности является использование персональных данных, без согласия субъектов, например, для проведения таргетированной рекламы или распространения спама. Это может привести к нарушению личной жизни и доверия пользователей в отношении информационных технологий.

Для защиты пользователей и предотвращения угроз информационно-психологической безопасности в открытых информационных системах необходимо проводить обучение конечных пользователей и укреплять технические меры защиты данных. Также необходимо улучшать законодательство и международное сотрудничество в сфере информационной безопасности.

Соблюдение правил поведения в сети является критически важным для личной и общественной безопасности в открытых информационных системах. С неправильным или небезопасным поведением пользователи рискуют не только своей личной информацией, но и могут стать источником угрозы для других пользователей, компаний или государств.

Например, то что пользователи выкладывают в социальных сетях может быть использовано для проведения атак на их личную жизнь и конфиденциальность. Кроме того, пользователи могут стать жертвами фишинговых атак и получить вредоносный код на своих устройствах, что может привести к утечке личной информации.

Когда пользователь рассылает спам или вирусы, это может замедлять работу всей сети, а также наносить ущерб компаниям и государственным учреждениям.

Для обеспечения личной и общественной безопасности в сети важно соблюдать правила поведения, такие как: не разглашать личную информацию в интернете, не открывать подозрительные вложения и ссылки, использовать сильные пароли и никогда их не давать другим людям, не выкладывать в сети информацию о других людях без их согласия, не поведение, не осуждать или не угрожать другим людям.

Соблюдение правил поведения в сети поможет уменьшить угрозы информационной безопасности и сохранить личную и общественную безопасность в открытых информационных системах.

Литература

1. Лунев А. Н., Пугачева Н. Б., Стуколова Л. З. Иформационно-психологическая безопасность личности: сущностная характеристика //Современные проблемы науки и образования. - 2014. - №. 1. - С. 21-21.
2. Краснянская Т. М., Тылец В. Г. Информационно-психологическая безопасность: угрозы личностному развитию и их преодоление //Развитие системы педагогического образования в современной России: антропологический аспект. - 2015. - С. 54-59.

3. Чемоданова М. В. Проблема информационно-психологической безопасности личности в современных психологических исследованиях //Вестник Марийского государственного университета. - 2017. - Т. 11. - №. 4 (28). - С. 98-104.
4. Яковлев И. И. Информационная безопасность как элемент системы безопасности социума //Научные проблемы гуманитарных исследований. - 2011. - №. 10. - С. 243-248.
5. Ватрушкин А. А. Проблемы информационно-психологической безопасности в современном мире //Актуальные проблемы гуманитарных и естественных наук. - 2010. - №. 11. - С. 193-197.
6. Шайдуллаев Н. Обеспечение информационно-психологической безопасности в открытых информационных системах //Теория и практика современной науки. - 2017. - №. 4. - С. 909-912.
7. Лызь Н. А., Веселов Г. Е., Лызь А. Е. Информационно-психологическая безопасность в системах безопасности человека и информационной безопасности государства //Известия Южного федерального университета. Технические науки. - 2014. - №. 8 (157). - С. 58-66.
8. Лепский В. Е. Информационно-психологическая безопасность субъектов дипломатической деятельности //Дипломатический ежегодник-2002: сборник статей колл. авторов. М.: Научная книга. - 2003. - С. 233.
9. Баранова Ю. М. и др. К вопросу об информационно-психологической безопасности детей и подростков в сети Интернет //Социальная психология и общество. - 2012. - Т. 3. - №. 4. - С. 122-129.
10. Пую Ю. В. Влияние информационно-психологической безопасности на конструктивное развитие России //Известия Российского государственного педагогического университета им. АИ Герцена. - 2009. - №. 104.
11. Ismoilov T. I. Provision of information-psychological security in open information systems //Теория и практика современной науки. - 2018. - №. 1. - С. 24-26.
12. Смирнов А. А. К вопросу о понятии, объекте и содержании информационно-психологической безопасности //Административное право и процесс. - 2013. - №. 1. - С. 34-38.
13. Вольнов Р. В. Психолого-правовые особенности обеспечения информационной безопасности личности //Акмеология. - 2010. - №. 2. - С. 34-38.
14. 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.