

Вопросы безопасности*Правильная ссылка на статью:*

Костюченко К.Л., Мухачев С.В. Оценка осведомленности студентов в сфере информационных технологий и информационной безопасности // Вопросы безопасности. 2024. № 2. DOI: 10.25136/2409-7543.2024.2.43491
EDN: JITEVB URL: https://nbpublish.com/library_read_article.php?id=43491

Оценка осведомленности студентов в сфере информационных технологий и информационной безопасности

Костюченко Константин Леонидович

кандидат технических наук

доцент, кафедра информационных технологий и защиты информации, Уральский государственный университет путей сообщения

620034, Россия, Свердловская область, г. Екатеринбург, ул. Колмогорова, 66

 kkost2@yandex.ru**Мухачев Сергей Валентинович**

кандидат физико-математических наук

доцент, кафедра Информационных технологий и защиты информации, Уральский государственный университет путей сообщения

620034, Россия, Колмогорова область, г. Екатеринбург, ул. Колмогорова, 66

 msv62@yandex.ru[Статья из рубрики "Человек и гражданин в системе безопасности"](#)**DOI:**

10.25136/2409-7543.2024.2.43491

EDN:

JITEVB

Дата направления статьи в редакцию:

03-07-2023

Дата публикации:

12-06-2024

Аннотация: Статья посвящена результатам изучения состояния осведомленности студентов в сфере информационных технологий. Предметом исследования являются

основные элементы информационных технологий и информационной безопасности. Изучались аспекты, связанные с применением информационных технологий, использованием методов защиты информации, пониманием характера информационных угроз обучающимися в образовательных организациях высшего образования. Объектом исследования являются различные образовательные учреждения, в т. ч. правоохранительные. Представлены результаты анкетирования студентов за несколько лет. Анализируются полученные данные по владению компьютерными технологиями, а также негативному информационному воздействию. Особое внимание уделяется сравнению с аналогичными данными, приведенными в других публикациях. Основными выводами проведенного исследования является то, что опрошенные респонденты активно используют информационные технологии в учебной работе, развлечениях, общении, однако, при этом, им достаточно слабо известны вопросы информационной безопасности. Молодое поколение неполно понимает степень опасности по отношению к обрабатываемой информации, собственному психическому и физическому здоровью, финансовому благополучию, а в некоторых случаях и жизни. Менее половины опрошенных осведомлены о требованиях нормативно-правовых актов в информационной сфере, из-за чего не используются даже самые обычные средства защиты информации. Из результатов анализа следует, что уровень осведомленности слабо меняется с течением времени.

Ключевые слова:

информационные технологии, информационная безопасность, кибербезопасность, компьютерная безопасность, Интернет, информационное воздействие, анкетирование, достоверность информации, компетенции, информационная война

Введение

В современном мире информационная сфера развивается очень стремительно – намного быстрее других сфер. Расширяются и качественно улучшаются функциональные возможности компьютерной и телекоммуникационной техники, появляются новые устройства и программы, совершенствуются мобильные системы связи, ускоряется обработка возрастающих данных, взрывообразно растет объем накапливаемых данных. Информационные технологии распространяются во все новые области. Если на заре развития компьютер применялся только для математических расчетов, то сегодня трудно назвать область, где бы он не использовался: документооборот, телекоммуникации, управление сложными техническими системами, работа с большими данными в различных сферах (банки, госуслуги), учебный процесс, игры и многие другие.

Наряду с несомненными положительными достижениями, связанными с информационными и телекоммуникационными технологиями, расширяется и круг проблем в сфере информационной безопасности. К «традиционным» угрозам безопасности (компьютерные вирусы, программы-шпионы, несанкционированный доступ к данным, средства модификации и уничтожения информации) добавляются различные варианты негативного информационного воздействия: спам, нежелательный контент, вульгарный и агрессивный характер общения в средствах коммуникации, кибермошенничество, геймизация сознания, навязывание криминального поведения, склонение к суициду и др. Особенno подвержена такому воздействию молодежь, том числе студенческая [\[1\]](#).

С целью противодействия негативным явлениям необходимо учитывать названные

негативные аспекты при разработке и преподавании учебных курсов по информационным технологиям и информационной безопасности. С этой целью требуется знать степень осведомленность студентов в указанных вопросах. Затем, на основе анализа полученных результатов, необходимо, на основе сложившегося состояния и оценки перспектив, своевременно вносить корректировки в образовательные стандарты и программы обучения [2, 3].

Подобные исследования систематически проводятся в различных странах: изучается осведомленность в вопросах компьютерной безопасности (кибербезопасности, веб-безопасности) [1, 4-7]; анализируется поведения подростков при виртуальном общении [3, 8]; исследуются различные педагогические аспекты обучения молодежи информационным технологиям и поддержанию информационной безопасности [2, 7, 9]. Поэтому интересно получить данные, относящиеся к Российским студентам, сравнить результаты их анализа с уже опубликованными, оценить сложившиеся реалии.

Методы и материалы

При выполнении работы использовались следующие методы: изучение материалов научных изданий по проблеме, наблюдение, анкетирование, теоретический анализ.

Данное исследование является логическим продолжением ранее проведенных работ:

- изучение компьютерной грамотности студентов и применения ими различных информационных технологий и технологий безопасности в государственных и частных высших учебных заведениях г. Екатеринбурга в 2006 г. (проведено анкетирование 593 студентов разных специальностей);
- изучение процессов информационного воздействия на курсантов и слушателей (заочной формы обучения) вуза МВД России в 2015 г. (проведено анкетирование 190 обучающихся).

Исследование продолжилось в 2019-2022 гг. на базе одного из технических вузов Урала. Цель – определить количественные характеристики компетенций, связанных с различными аспектами использования информационных технологий и информационной безопасности.

Анкетирование выполнялось анонимно. Сбор материалов реализован в два этапа. На первом этапе в сплошном анкетировании приняли участие 360 студентов первого курса (технические специальности, очная форма обучения). Дополнительно, на втором этапе, методом случайного отбора был проведен выборочный опрос 22 студентов 3-го курса и 30 студентов заочной формы обучения.

В анкете использовались вопросы из анкет предыдущих исследований и некоторые другие, специально разработанные.

Анкеты включали два блока вопросов, а также информацию о возрасте и специальности, по которой обучается студент. Первый блок содержал вопросы, касающиеся применения информационных технологий опрашиваемыми студентами. Респондентам предлагалось оценить свой уровень знаний информационных технологий в целом; уровень знаний офисных компьютерных программ; удовлетворенность используемыми операционными системами и отдельными прикладными программами; необходимость изучения некоторых новых программ; уровень владения мобильными технологиями.

Второй блок содержал вопросы по тематике информационной безопасности. Вопросы были сформулированы следующим образом.

«Сколько времени в день Вы проводите в Интернет, не считая учебы (в часах)?»

«Играете ли в компьютерные игры (если да, то насколько много (в часах)?»

«Оцените: какова достоверность информации в Интернете (%)?»

«Оцените: каковы Ваши познания в вопросах информационной безопасности (%)?»

«Считаете ли Вы, что против Вас идет информационная (психологическая, информационно-психологическая) война?»

«Считаете ли Вы свои персональные данные защищенными?»

«Пользуетесь ли Вы антивирусной программой? Если – да, то – какой?»

«Выполняете ли требования нормативно-правовых актов в информационной сфере?»

«Какие информационные воздействия за последнее время повлияли на Ваши взгляды, действия, учебу?»

«Владеете ли Вы приемами противодействия негативным результатам информационного воздействия?»

Результаты

Собранный в результате анкетирования материал был обработан с использованием стандартных статистических методов.

Средний возраст опрошенных составил 18 лет. 38% респондентов – девушки.

Свой уровень владения информационными технологиями студенты оценили значением 65%, а мобильными технологиями – 87%. Уровень знаний отдельных программ популярного пакета Microsoft Office представлен на рис. 1. Программированием занимается 1 % опрошенных, но 5 % желают изучить программирование более глубоко, а 9 % – изучить системы управления базами данных.

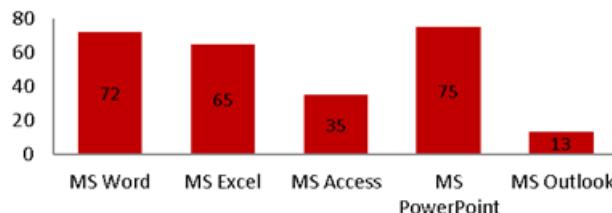


Рис. 1. Данные об оценке студентами уровня знаний отдельных программ популярного пакета Microsoft Office (в процентах)

Другие наиболее значимые результаты обработки анкет сведены в таблице 1 и наглядно представлены на рис. 2 и 3.

Таблица 1. Основные результаты анкетирования студентов

Характеристика	Значение
Среднее время, проведенное в Интернет, не считая учебы, час/день	6,3

Среднее время, затраченное на компьютерные игры, час/день	1,7
Доля респондентов, считающих, что информация в Интернете полностью достоверна, %	58
Степени компетентности в сфере информационной безопасности (оценка респондентов), %	44
Оцененный вклад тематики компьютерной безопасности в информационной безопасности (оценка респондентов), %	52
Доля респондентов, считающих, что их персональные данные защищены, %	38
Доля респондентов, которые не пользуются антивирусными программами, %	25
Доля ответов «Против Вас идет информационная война», %	23

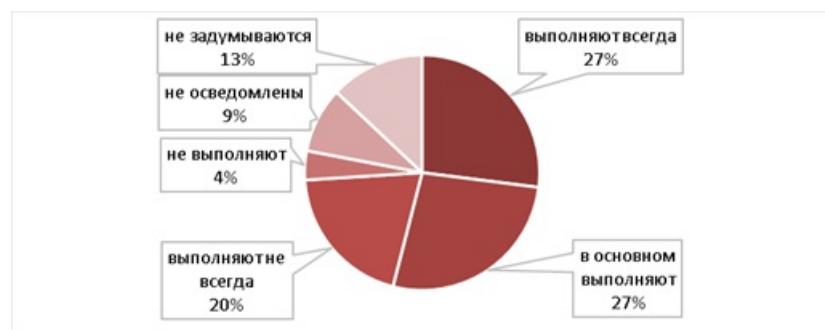


Рис. 2. Данные о выполнении студентами требований нормативно-правовых актов в сфере информационных технологий и информационной безопасности

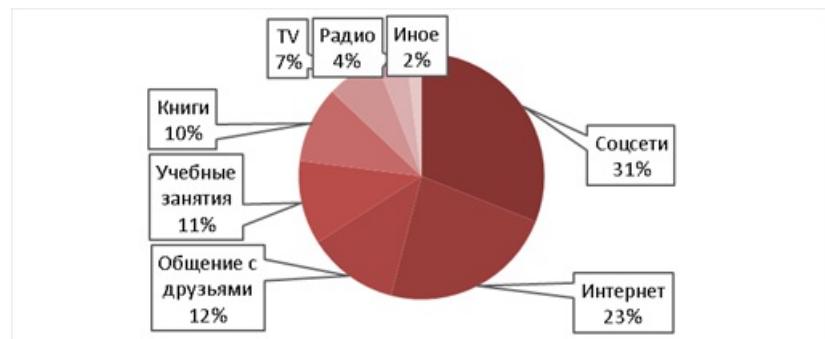


Рис. 3. Структура источников информации студентов

Обсуждение

Анализ полученных данных и сравнение их с аналогичными исследованиями позволяют сформулировать следующие выводы.

- Студенты очень много времени проводят за компьютером – в среднем более 6 часов в день (данные получены до ограничений, связанных с пандемией COVID). Из них примерно 2 часа – за компьютерными играми. Из результатов анкетирования можно видеть, что девушки в компьютерные игры играют гораздо меньше (2-3% опрошенных), чем юноши. Поэтому реальное значение времени, приходящееся на компьютерные игры, превышает 4 часа. Это серьезная проблема, так как столь длительное время, уделяемое играм, негативно сказывается на физическом здоровье молодых людей. В отдельных ситуациях может проявляться криминальное поведение, а также психические отклонения

[\[2, 10\]](#). При дистанционной форме обучения проблема, связанная с чрезмерной длительностью использования компьютера только усугубляется.

2. Основным источником информации является Интернет и соцсети (54 % опрошенных). И это при том, что достоверность информации в сети Интернет самими опрошенными оценивается лишь в 58 %, а экспертами она оценивается еще ниже – 15-25 %. В самом деле, многие исследователи приводят многочисленные факты появления фейковых новостей, распространения дезинформации, манипулирования в социальных сетях и иных источниках цифрового пространства [\[11, 12\]](#). Эти значения вполне согласуются с данными, полученными ранее при анкетировании курсантов и слушателей правоохранительного вуза.

3. Недавние выпускники общеобразовательных организаций довольно слабо осведомлены в вопросах информационной безопасности (лишь 44 %). Только 23 % опрошенных считают, что против них лично идет информационная война. Примерно такое же количество студентов признают существование информационного противоборства, но к себе этот факт не относят. Это давняя проблема формирования общей культуры безопасности, связанная в основном с недостатками преподавания исторических и общественно-политических дисциплин.

Следует отметить, что опрошенные не отождествляют понятие «информационная безопасность» и «компьютерная безопасность», несмотря на наблюдаемое смешение этих понятий в подавляющем большинстве средств массовой информации и в других источниках. Условно считают, что тематика компьютерной безопасности составляет только около половины общей тематики информационной безопасности.

4. Требования нормативно-правовых актов в информационной сфере соблюдает (в той или иной степени) лишь около половины студентов, а около четверти о правовых аспектах и их выполнении не осведомлены или не задумываются об этом.

5. Следствием неосведомленности и, отчасти, невыполнением нормативно-правовых актов (правовой нигилизм), является то, что почти четверть анкетируемых не пользуются антивирусными программами, т.е. никак не защищает свою компьютерную информацию. Возможно, имеет место и обычное нежелание тратиться (из-за ограниченности в ресурсах). Представляется, что эти же утверждения справедливы и для других тематик компьютерной безопасности.

6. Только около половины опрошенных респондентов ответили, что владеют приемами противодействия негативным результатам информационного воздействия. Однако с этой цифрой сложно согласиться, т. к. она кажется завышенной (может быть из-за непонимания сложности тематики). Источники отрицательного информационного влияния существуют в большом количестве, часто в неявном виде. Это инструменты информационно-психологической войны: активная дезинформация, экстремистские призывы, непроверенные новости, слухи, сплетни, злобные карикатуры, демотиваторы и др. Подобная информация, крайне негативно влияет на сознание человека, его мировоззрение, а, следовательно, его поведение и конкретные действия. Результатом могут стать различные фобии, привязанности, зависимости, различные расстройства, неадекватные потребности и т. п. От этого нужно уметь защищаться. Для сравнения – всего лишь около 15 % курсантов и слушателей правоохранительного вуза, участвовавших ранее в анкетировании, показали, что предпринимают хоть какие-либо конкретные меры по снижению негативных информационных воздействий и минимизации их последствий. И это при том, что с сотрудниками правоохранительных органов ведется

плановая воспитательная и психологическая работа. Но четких соответствующих методик (прежде всего, психологических) пока не хватает.

Выводы

В результате проведенного исследования получены интересные результаты, позволяющие судить об осведомленности студентов в различных аспектах информационных технологий, их применении и информационной безопасности. Несмотря на достаточной длинный временной период, прошедший с момента первого анкетирования, основные особенности, которые выявляются в результате анкетирования в студенческой среде, изменяются слабо. Результат достаточно интересный, так как стремительно меняется все: технический уровень информационных технологий, степень освоения технических и программных средств, учебные программы образовательных учреждений. Можно, по-видимому, сделать вывод о наличии (а, возможно, и преобладании) консервативных психологических факторов, влияющих на состояние изучаемой предметной области.

Результаты исследования позволяют судить о состоянии осведомленности студентов в сфере информационных технологий и информационной безопасности. Получены количественные показатели, характеризующие владение информационными технологиями и методами информационной безопасности, характеризующие основные источники информации в студенческой среде, отношение к нормативно-правовому регулированию изучаемой в работе области. Выявленные особенности необходимо использовать при подготовке и совершенствовании учебных планов и рабочих программ, регламентирующих образовательный процесс.

Библиография

1. Chusavitina, G.N., Zerkina, N.N., Makashova, V.N. Special aspects of future teachers' training in ensuring information security sphere for university students // Перспективы науки и образования 2018. 35(5). С. 259-266.
2. Курзаева Л.В., Чусавитина, Г.Н. К вопросу о формировании требований к компетенциям личности в области информационной безопасности в системе высшего профессионального образования // Фундаментальные исследования 2013. № 8-5. С. 1203-1207.
3. Чусавитина, Г.Н., Мусийчук М.В. Педагогические проблемы противодействия угрозам в сети Интернет // Интернет-журнал «Мир науки». 2017. Т. 5. № 6. С. 1-14.
4. Арутюнов В.В. Об Интернет-ресурсах для пользователей // Вестник МФЮА № 1/2013 С. 79-84.
5. Chan, R.Y.-Y., & Ho, K.M., & Jia, S., & Yan, X., & Yu, X. (2017). *Facebook and information security education: What can we know from social network analyses on Hong Kong engineering students?* Proceedings of 2016 IEEE International Conference on Teaching, Assessment and Learning for Engineering, TALE 2016.
6. Alharbi, T., & Tassaddiq, A. (2021). *Assessment of cybersecurity awareness among students of Majmaah University.* Big Data and Cognitive Computing 5(2), 23.
7. Cruz, T., & Simões, P. (2020). *Fostering cybersecurity awareness among computing science undergraduate students motivating by example.* European Conference on Information Warfare and Security, ECCWS 2020. June, pp. 72-81.
8. Nowrin, S., & Bawden, D. (2018). *Information security behaviour of smartphone users: An empirical study on the students of university of Dhaka, Bangladesh.* Information and Learning Science 119(7-8), pp. 444-455.
9. Wu, T., & Tien, K.-Y., & Hsu, W.-C., & Wen, F.-H. (2021). *Assessing the effects of*

gamification on enhancing information security awareness knowledge. Applied Sciences (Switzerland) 11(19), 9266.

10. О дифференциации ответственности при проведении бинарных опционов с использованием «биржевых терминалов» в контексте предупреждения преступности и игромании несовершеннолетних / Макаренко Т.Д., Смирнов А.М., Санташов А.Л., Миронов А.В., Некрасов В.Н. // Всероссийский криминологический журнал. 2018. № 12 (6) С. 856-864.

11. Hilary, I.O., & Dumebi, O.-O. (2021). *Social media as a tool for misinformation and disinformation management. Linguistics and Culture Review* 5, pp. 496-505.

12. Caramacion, K.M. (2020). An exploration of disinformation as a cybersecurity threat. Proceedings-3rd International Conference on Information and Computer Technologies, ICICT 2020 9092330, pp. 440-444.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться [здесь](#).

На рецензирование представлена работа «Оценка осведомленности студентов в сфере информационных технологий и информационной безопасности».

Предмет исследования. Предмет исследования в работе не обозначен, но работа посвящена исследованию оценки осведомленности студентов в сфере информационных технологий и информационной безопасности. В целом, можно отметить, что предмет в работе раскрыт полностью. Автор разграничил и уточнил понятия, выделил необходимые феномены и рассмотрел основных подходы к их рассмотрению. Несмотря на небольшую выборку, результаты были получены достоверные.

Методология исследования. Автором было проведено исследование с использованием ряда методов (изучение материалов научных изданий по проблеме, наблюдение, анкетирование, теоретический анализ.).

Автором было проведено исследование, целью которого было определение количественных характеристик компетенций, связанных с различными аспектами использования информационных технологий и информационной безопасности.

В исследовании приняло участие 360 студентов первого курса, которые обучаются по очной форме обучения на технических специальностях.

В основу анкеты были положены следующие вопросы:

Первый блок содержал вопросы, касающиеся применения информационных технологий опрашиваемыми студентами. Респонденты оценивали свой уровень знаний информационных технологий в целом; уровень знаний офисных компьютерных программ; удовлетворенность используемыми операционными системами и отдельными прикладными программами; необходимость изучения некоторых новых программ; уровень владения мобильными технологиями.

Второй блок состоит из вопросов по тематике информационной безопасности.

Актуальность исследования не вызывает сомнения. Автором обосновывается актуальность затронутой проблематики с позиции общественного запроса и дефицитарности имеющихся исследований.

Научная новизна.

Автором были получены следующие результаты:

выявлена длительность времени проведения за компьютером, особенности отношения мужчин и женщин;

выделены основные источники информации для молодых людей и особенности

осведомленности молодых людей по вопросам информационной безопасности; выявлены особенности владения приемами противодействия негативным результатам информационного воздействия.

Стиль, структура, содержание. Стиль изложения соответствует публикациям такого уровня. Язык работы научный.

Структура работы четко прослеживается. Во введении представлено описание актуальности исследования, выделены основные проблемы и трудности. Во втором разделе «Методы и материалы» представлено описание методов, выделены предыдущие этапы проведенных работ. Особое внимание удалено описанию применяемых методик и основных его блоков. Третий раздел посвящен описанию полученных результатов. Следующий раздел является основным, который посвящен описанию обсуждения полученных результатов и выводов. Заканчивается статья краткими выводами.

Библиография. Библиография статьи включает в себя 12 отечественных и зарубежных источников, менее половины которых было издано за последние три года. В списке представлены научно-исследовательские статьи, монографии. На оформление источников информации необходимо обратить внимание, не все оформлены корректно.

Апелляция к оппонентам.

Поставленные автором цель и задачи реализованы. Однако, есть моменты, которые требуют дополнения:

- провести анализ современных исследований, поскольку теоретический является недостаточным;
- выводы прописать более подробно, уделив внимание научной новизне проведенного исследования и личностному вкладу автора.

Выводы. Проблематика статьи отличается несомненной актуальностью, теоретической и практической ценностью, будет интересна исследователям. Работа может быть рекомендована к опубликованию.