Электронный научный журнал «Век качества» ISSN 2500-1841 http://www.agequal.ru

2021, №1 http://www.agequal.ru/pdf/2021/AGE_QUALITY_1_2021.pdf

**Ссылка для цитирования этой статьи:**

Поначугин А.В., Тимофеева К.О., Зайцева М.Р. Обоснование эффективности использования методов сохранения и защиты информации пользователей компьютерных систем // Электронный научный журнал «Век качества». 2021. №1. С. 76-96. Режим доступа: http://www.agequal.ru/pdf/2021/121005.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 004.056.5

# Обоснование эффективности использования методов сохранения и защиты информации пользователей компьютерных систем

***Поначугин Александр Викторович,***
*кандидат экономических наук, доцент кафедры Прикладной информатики и информационных технологий в образовании, Нижегородский государственный педагогический университет имени К. Минина,*
*Россия, 603005, г. Нижний Новгород, ул. Ульянова, 1*
*sasha3@bk.ru*

***Тимофеева Ксения Олеговна***
*студентка, Нижегородский государственный педагогический университет имени К. Минина,*
*Россия, 603005, г. Нижний Новгород, ул. Ульянова, 1*
*kceni_21_01_99@mail.ru*

***Зайцева Мария Романовна***
*студентка, Нижегородский государственный педагогический университет имени К. Минина,*
*Россия, 603005, г. Нижний Новгород, ул. Ульянова, 1*
*zaitsevamasha1999@mail.ru*

Рассмотрены виды информации, инструменты и области, используемые для ее защиты, а также проведен опрос среди обучающихся по IT специальности НГПУ им. Козьмы Минина.

В ходе выполнения работы были использованы следующие методы: методы теоретического исследования (теоретический анализ и синтез, абстрагирование и конкретизация, изучение специализированной литературы); статистические методы: математическая обработка данных, полученных в ходе проведения опроса.

Проведено онлайн-тестирование среди будущих специалистов в сфере IT-технологий. Анализирование результатов показало, что даже они сталкиваются с разными угрозами информационной безопасности, такими

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

как утечка конфиденциальной информации, заражение системы компьютерными вирусами, кража личных аккаунтов и т.д. По итогам проведенного исследования и анализа полученных результатов опроса в рамках данной статьи описаны, какие технологии защиты информации необходимо использовать. Предложенные технологии защищенности важных свойств сети интернет, таких как конфиденциальность, целостность и доступность защищенных ресурсов, могут применяться как обычными пользователями интернета, так и организациями, предприятиями, крупными компаниями и т.д. Данное исследование может служить теоретической основой в формировании представления об актуальных проблемах информационной безопасности. Предложенный комплекс мер по защите информации направлен на борьбу с выявленными угрозами, с которыми чаще всего сталкиваются пользователи. Данный комплекс может быть использован на различных предприятиях с целью повышения уровня информационной защищенности.

**Ключевые слова:** безопасность, информация, интернет, киберпреступник, защита, угроза, уязвимости, кибербезопасность.

## Введение

Информационная безопасность обеспечивает защиту инфраструктуры данных и сетей, которые содержат конфиденциальную, частную, финансовую и корпоративную информацию, а также затрагивает область исследования кибернетической экспертизы, защиты мобильных вычислений и социальных сетей в Интернете [1]. Она позволяет людям защищать свою цифровую и аналоговую информацию от несанкционированного доступа, использования в корыстных целях, раскрытия, нарушения, модификации, проверки, записи или уничтожения. В свою очередь, кибербезопасность борется с киберпреступностью и защищает как необработанные, так и значимые объемы данных, но только уже от различных интернет-угроз в киберпространстве.

Основные цели защиты информационных ресурсов обычно строятся на обеспечении конфиденциальности, целостности и доступности информации любого пользователя.

**Конфиденциальность** предотвращает несанкционированный доступ к информации для защиты личного информационного содержания. Она поддерживается за счет ограничений доступа и строгой идентификации личности пользователя, а ее нарушение может произойти как из-за человеческой ошибки, так и из-за преднамеренного обмена или злонамеренного входа [2].

**Целостность** обеспечивает достоверность и точность информации. Она поддерживается с помощью ограничения разрешений на возможность редактирования или изменения информации. Потеря целостности может произойти, когда:

- аналоговая информация не защищена от условий окружающей среды;
- цифровая информация не передаётся должным безопасным образом;
- пользователи вносят несанкционированные изменения.

**Доступность** гарантирует, что авторизованные пользователи могут получить надежный доступ к информации. Она поддерживается за счет непрерывности процедур доступа, резервного копирования в облачные сервисы или внешние носители и дублирования информации, а также беспрерывного обслуживания оборудования и сетевых подключений. Потеря доступности может произойти, когда сети атакованы стихийными бедствиями или, когда пользовательские устройства выходят из строя [3].

Научная новизна результатов исследования заключается в следующих моментах:

- выявлен уровень осведомленности студентов НГПУ им. Козьмы Минина г. Нижнего Новгорода об угрозах информационной безопасности и их устранения, на основе чего построена исследовательская часть статьи;

- даны рекомендации по улучшению обеспечения информационной безопасности при помощи соблюдения предложенного авторами комплекса мер по защите информации;
- получены данные о восприятии проблем информационной безопасности на различных организационных уровнях.

Актуальность исследуемой области обусловлена тем, что информация является самым ценным ресурсом для каждой сферы жизни, тем самым способствуя мотивации быть украденной, искаженной и раскрытой киберпреступниками и злоумышленниками. Следовательно, для того, чтобы обезопасить информацию от различных видов угроз, необходимо уметь правильно применять комплексный подход к защите своих данных.

Данная тема уже была затронута в работах многих специалистов в сфере информационной безопасности. Например, Н.В. Скабцов в своей книге «Аудит безопасности информационных систем» [4] рассматривает методы обхода систем безопасности сетевых сервисов и проникновения в открытые информационные системы. А Р.И. Захарченко и И.Д. Королев описали функционирование критической информационной инфраструктуры (КИИ) в киберпространстве, порождающее новые уязвимости и угрозы, и требующее разработки нового инструментария обеспечения безопасности, в своей публикации «Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве» [5].

Постановка проблемы заключается в пренебрежении пользователями интернета правилами информационной безопасности. В основном люди пользуются стандартными, но слабыми способами информационной защиты. Простой и легко запоминающийся пароль, передача незашифрованных данных, переход по подозрительным ссылкам и публикация персональных данных в различных соц. сетях и общедоступных сайтах являются главными уязвимостями сетевой деятельности пользователя, которыми

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

злоумышленники легко пользуются. Большинство людей не осведомлены о более надежных методах защиты и не применяют их на практике, что делает их потенциальными жертвами компьютерных атак.

Проблематика была выявлена в результате исследования путем проведения онлайн-опроса среди будущих специалистов в сфере IT-технологий. Анализирование результатов показало, что даже они сталкиваются с разными угрозами информационной безопасности, такими как утечка конфиденциальной информации, заражение системы компьютерными вирусами, кража личных аккаунтов и т.д. Таким образом, можно сказать, что целью исследования является выявление умения людей бороться с проблемой угроз киберпространства и компьютерных атак.

Поскольку информационная безопасность охватывает множество областей для защиты информации, она часто включает в себя реализацию различных типов безопасности, включая безопасность приложений, инфраструктуры, криптографию, реагирование на угрозы, управление уязвимостями и аварийное восстановление [6].

## Типы информационной безопасности

При рассмотрении информационной безопасности выделяют множество подтипов. Эти подтипы охватывают определенные виды информации, инструменты и области, используемые для защиты информации.

- *Безопасность приложений*

Стратегии безопасности приложений используются для предотвращения, обнаружения и исправления ошибок или других уязвимостей в приложениях, иначе они могут стать шлюзом для более широких систем, подвергая информацию риску.

Безопасность приложений во многом основана на специализированных инструментах для защиты, сканирования и тестирования программ. Эти

инструменты помогают определить уязвимости в приложениях и окружающих компонентах [7]. После обнаружения таковых можно исправить эти уязвимости до их использования или до выпуска приложений.

- *Безопасность инфраструктуры*

Стратегии безопасности инфраструктуры защищают ее компоненты, включая сети, серверы, клиентские устройства, мобильные устройства и центры обработки данных. Растущая взаимосвязь между этими и другими компонентами подвергает информацию риску без надлежащих мер предосторожности.

Этот риск связан с тем, что возможность подключения увеличивает уязвимости в системах. Если одна часть инфраструктуры выходит из строя или скомпрометирована, это также затронет все её зависимые компоненты. В связи с этим важной целью безопасности инфраструктуры является минимизация зависимостей и изоляция компонентов, сохраняя при этом возможность взаимодействия.

- *Облачная безопасность*

Облачная безопасность обеспечивает защиту, аналогичную защите приложений и инфраструктуры, но ориентирована на облачные или подключенные к облаку компоненты и информацию. Облачная безопасность добавляет дополнительные средства защиты и инструменты, позволяющие сосредоточить внимание на уязвимостях, исходящих от служб с выходом в Интернет и общих сред, таких как общедоступные облака. Она также имеет тенденцию [8] включать в себя централизацию управления безопасностью и инструментов. Такая централизация позволяет поддерживать видимость информации и информационных угроз в распределенных ресурсах.

Другой аспект облачной безопасности - это сотрудничество с облачным провайдером или сторонними сервисами. При использовании ресурсов и приложений, размещенных в облаке, можно полностью контролировать свои среды, поскольку инфраструктура обычно управляется

сама. Это означает, что в практике облачной безопасности необходимо учитывать ограниченный контроль и принимать меры для ограничения доступности и уязвимостей, исходящих от подрядчиков или поставщиков.

- *Криптография*

Криптография использует метод, называемый шифрованием, для защиты информации, скрывая ее содержимое. Когда информация зашифрована, она доступна только пользователям, имеющим правильный ключ [4]. Команды безопасности могут использовать шифрование для защиты конфиденциальности и целостности информации на протяжении всего срока ее службы, в том числе при хранении и во время передачи. Однако, как только пользователь расшифровывает данные, они становятся уязвимыми для кражи, раскрытия или изменения.

Для шифрования информации группы безопасности используют такие инструменты, как алгоритмы шифрования или такие технологии, как блокчейн. Алгоритмы шифрования по типу расширенного стандарта шифрования (AES), более распространены, поскольку для этих инструментов больше поддержки и меньше накладных расходов на использование.

- *Реагирование на угрозы*

Реагирование на угрозы представляет собой набор процедур и инструментов, которые можно использовать для выявления, расследования и обнаружения атак или разрушительных событий. Оно устраняет или уменьшает ущерб, причиненный системам из-за атак, стихийных бедствий, сбоев системы или человеческой ошибки.

Обычно используется система автоматизации реагирования на инциденты информационной безопасности (IRP), которая определяет роли и обязанности по отклику на инциденты. Эта система также определяет политику безопасности [9], содержит руководящие принципы или процедуры для действий и помогает обеспечить использование информации, полученной в результате угроз, для улучшения защитных мер.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

- *Управление уязвимостями*

Управление уязвимостями - это практика, предназначенная для снижения рисков, присущих приложению или системе. Идея этой практики заключается в обнаружении и исправлении уязвимостей до того, как проблемы будут обнаружены или использованы. Чем меньше уязвимостей в компоненте или системе, тем в большей безопасности находятся информация и ресурсы.

Практика управления уязвимостями основана на тестировании, аудите и сканировании системы для обнаружения проблем. Эти процессы часто автоматизируются, чтобы гарантировать, что компоненты оцениваются в соответствии с определенным стандартом и что уязвимости будут обнаружены как можно быстрее. Другой метод, который можно использовать, это охота за угрозами, включающий в себя исследование систем в режиме реального времени для выявления признаков угроз или поиска потенциальных уязвимостей.

- *Аварийное восстановление*

Стратегии аварийного восстановления защищают организацию от потерь или повреждений в результате непредвиденных событий. Они обычно учитывают, как можно восстановить информацию, как восстановить системы и как возобновить работу [10-11]. Эти стратегии часто являются частью плана управления непрерывностью бизнеса, разработанного, чтобы позволить организациям поддерживать операции с минимальным временем простоя.

Как было отмечено выше, компьютерные атаки развиваются намного быстрее, чем раньше, и несут за собой достаточно сильную угрозу. Следовательно, необходимо использовать целый комплекс мер по защите информации и данных, так как один инструмент обеспечения безопасности не всегда в одиночку может справиться со всеми выявленными угрозами. Для того, чтобы понять, какой комплекс мер нужно использовать, необходимо

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

определить, с как часто и с какими проблемами информационной безопасности чаще всего сталкиваются пользователи.

## Исследование и анализ полученных результатов

В целях исследования данной темы был проведен онлайн-опрос, который направлен на выявление умений обеспечить надежную защиту данных и с какими проблемами информационной безопасности чаще всего сталкиваются пользователи интернета. Участниками опроса являлись студенты НГПУ им. Козьмы Минина, обучающиеся по IT-специальности. Всего опрос прошли 102 человека, из которых 24,5% учатся на 1-м курсе, 24,5% - на 2-м курсе, 24,5% - на 3-м курсе и 26,5% - на 4-м курсе (рис. 1).


Рис. 1. Распределение респондентов по курсам обучения

Ответы на второй вопрос «Какие угрозы наиболее опасны, по Вашему мнению, для информационной безопасности?», помогли понять, какие проблемы информационной безопасности сейчас актуальны. Пользователи считают, что самыми опасными являются такие угрозы, как кража информации (73,5%), вредоносные программы (64,7%), аппаратные и программные сбои (62,7%) и финансовое мошенничество (62,7%) (рис. 2).

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

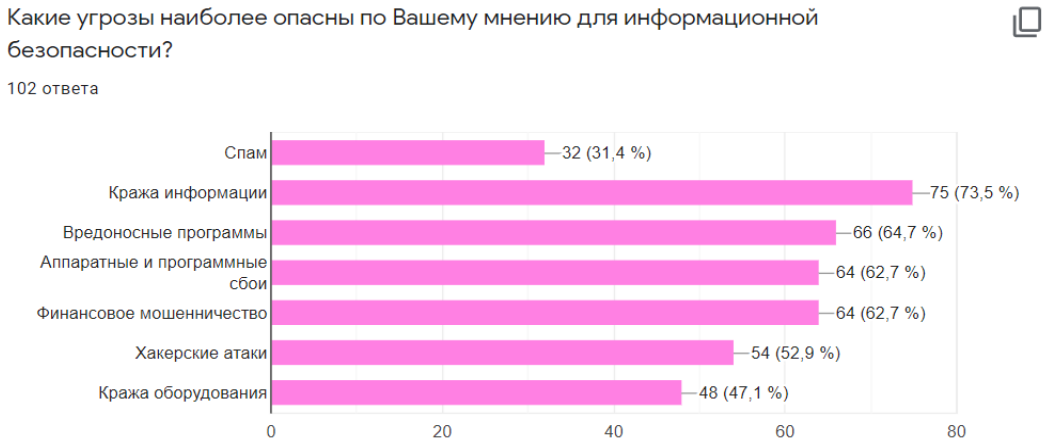


Рис. 2. Наиболее опасные угрозы по мнению респондентов

Также необходимо было выявить, как часто респонденты сталкиваются с различными угрозами информационной безопасности. Третий вопрос звучал так: «Сколько раз Ваш компьютер заражался вирусом или подвергался компьютерным атакам?». На него были даны следующие ответы:

- 35,3% - много (более двух раз),
- 30,4% - пару раз,
- 21,6% - один раз,
- 12,7% - ни разу.

Статистика ответов показала, что всего лишь 12,7% опрашиваемых ни разу не сталкивались с вирусами и компьютерными атаками, а остальные 87,3% один или более раз подвергались угрозам. Это говорит о том, что большой процент пользователей не умеет грамотно и надёжно выстраивать систему защиту своих данных (рис. 3).

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru


Рис. 3. Частота столкновения с компьютерными атаками и вирусами

Помимо того, что пользователи интернета подвергаются атакам с целью кражи личной информации, чаще всего люди сами выкладывают какие-либо данные о себе в социальные сети, что даёт злоумышленникам легкий доступ к этим данным. Но ответы на заданный вопрос «Беспокоит ли Вас публикация личной информации в соц. сетях?» говорят о том, что большинство респондентов обеспокоены тем, что их частная жизнь находится в общем доступе (62,7%), остальная часть не задумывается об этом (37,3%) (рис. 4).


Рис. 4. Отношение респондентов к публикации личной информации в сети

На пятый вопрос «Как Вы думаете можно ли в современном мире обойтись без антивирусной программы на своем компьютере?» большинство респондентов ответили, что нельзя обойтись без использования

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

антивирусного ПО (программного обеспечения) (58,8%), оставшаяся часть считает, что можно спокойно обойтись и без этого (41,2%) (рис. 5).

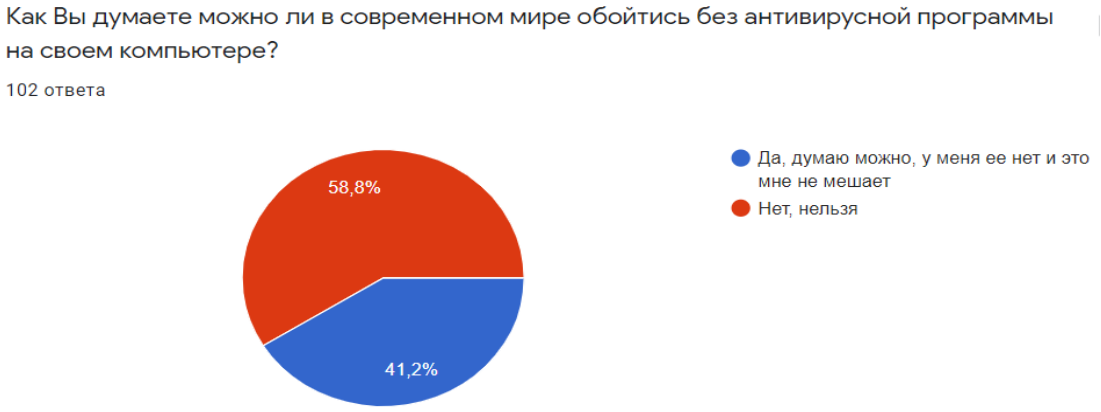


Рис. 5. Мнение респондентов об использовании антивирусных программ

Шестой вопрос «Пользуетесь ли Вы лицензионными средствами защиты информации?» вытекает из предыдущего. 58,8% опрашиваемых студентов ответили, что используют нелицензионное ПО для защиты, оставшиеся респонденты (41,2%) готовы платить за лицензионные средства защиты (рис. 6).

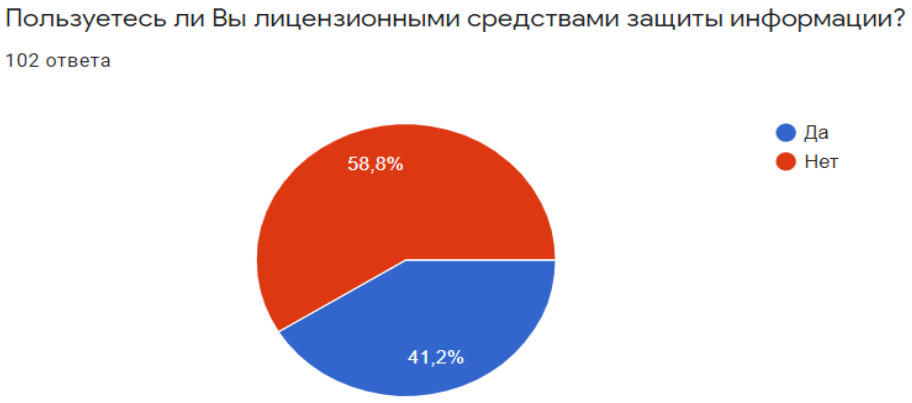


Рис. 6. Использование лицензионных средств защиты информации

Такие результаты отрицательного отношения к использованию лицензионного антивирусного ПО скорее всего связаны с тем, что подписка на лицензию продукта стоит достаточно дорого и не является долгосрочной, обычно она оформляется на месяц или год, по истечению этого срока

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

необходимо снова платить за активацию [12]. Также немаловажным аспектом может являться то, что антивирусы блокируют доступ ко многим ресурсам и не дают возможности установить «пиратские» программы.

Одним из важных вопросов данного опроса является вопрос «С какими угрозами Вы уже лично сталкивались?». Наиболее частыми угрозами являются:

- взлом личных аккаунтов - 62,7%;
- загрузка вредоносных ПО - 58,8%;
- модификация данных сторонними лицами (искажение, удаление, редактирование информации) - 56,9%;
- шантаж и вымогательство со стороны кибепреступников- 54,9%;
- взлом с целью нарушения работы системы - 52,9%.

Компьютерные атаки (49%) и кража личных данных (48%) - самые редкие угрозы, с которыми столкнулись респонденты (рис. 7).


Рис. 7. Угрозы, с которыми сталкивались опрашиваемые студенты

В результате проведенного опроса было важно узнать, какие методы и способы защиты информации применяют опрашиваемые студенты на своей практике. На последний вопрос «Что Вы делаете для того, чтобы обезопасить свои данные?» частыми ответами были самые простые и распространенные способы:

- использую надежные пароли - 71,6%;

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

- не храню ключи и пароли в файлах TXT, DOC, RTF и других документов на самом ПК - 69,6%.

Самыми непопулярными методами среди опрашиваемых являются:

- применение шифрования данных - 59,8%;
- отключение общего доступа к файлам на ПК по локальной сети, чтобы защитить Wi-Fi - 58,8%;
- использование антивирусных программ - 55,9%;
- установка пароля на BIOS и/или жесткий диск - 43,1%;
- использование встроенного защитника WIN10 - 1%.

Такие способы не особо популярны, так как они являются более продвинутыми и малоизвестными, и даже будущие IT-специалисты редко применяют их, так как обычно дисциплины по информационной безопасности изучаются на последнем курсе (рис. 8).

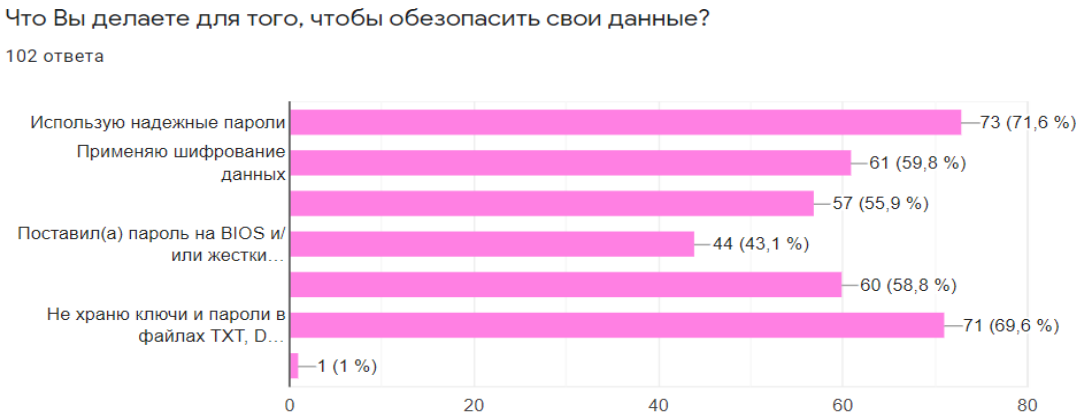


Рис. 8. Способы защиты данных респондентов

Анализ результатов исследования выявил, что большая часть опрашиваемых специалистов в сфере IT были атакованы компьютерными вирусами хотя бы один раз. Причина этому вытекает из ответов на последний вопрос, который показал, что используются в основном самые примитивные методы защиты и игнорируются более надежные, в частности использование антивирусных программ. Но стоит заметить, что многие

студенты так или иначе интересуются, как можно надежно защитить свои данные, и пользуются одновременно несколькими способами обеспечения информационной безопасности, объединяя их в один общий комплекс мер по защите информации.

## Применение технологий информационной безопасности

На сегодняшний день существует множество методов по обеспечению информационной безопасности, которые в совокупности могут создать сильную и надежную защиту данных.

Для борьбы с выявленными в результате исследования угрозами, с которыми сталкиваются пользователи, был составлен комплекс мер по защите информации. Создание эффективной стратегии информационной безопасности требует применения различных технологий и инструментов. В предлагаемой стратегии используется комбинация следующих технологий:

- *Брандмауэры* - это уровень защиты, который можно применять к сетям или приложениям. Эти инструменты позволяют фильтровать трафик и сообщать его данные в системы мониторинга и обнаружения. Это программа, главная функция которой - защита операционной системы от сетевых, хакерских атак. Назначение брандмауэра - выслеживать и блокировать все вредоносные подключения, обеспечивать защиту персональной пользовательской информации. То есть он постоянно прослушивает порты компьютера, чтобы выявить момент подключения к ним нехороших прог, вирусов, червей.

Каковы функции такой защиты:

1) следит за сомнительными соединениями, например, если они пытаются отправить информацию в Интернет;

2) блокирует порты, которые не участвуют в работе, и изучает трафик с открытых портов [14];

3) наблюдает за работающими приложениями и предупреждает пользователя, если изменяется важная информация запущенных прежде программ;

- *Управление угрозами и событиями безопасности (SIEM).* SIEM-решения позволяют получать и сопоставлять информацию из разных систем. Такое агрегирование данных позволяет группам более эффективно обнаруживать угрозы, управлять предупреждениями и обеспечивать лучший контекст для расследований. Решения SIEM также полезны для регистрации событий, происходящих в системе, или составления отчетов о событиях и производительности. Так же можно использовать эту информацию для подтверждения соответствия или оптимизации конфигураций;
- *Предотвращение потери данных (DLP).* Стратегии DLP включают инструменты и методы, которые защищают данные от потери или изменения. Это включает в себя категоризацию данных, резервное копирование и мониторинг обмена информацией внутри и за пределами локальной сети;
- *Система обнаружения вторжений (IDS).* Решения IDS - это инструменты для обнаружения угроз и мониторинга входящего трафика, который оценивается инструментами, предупреждающими о любых случаях, которые кажутся подозрительными или вредоносными;
- *Система предотвращения вторжений (IPS).* IPS-решения аналогичны решениям IDS, и они часто используются вместе. Эти решения реагируют на трафик, который определяется как подозрительный или вредоносный, блокируя запросы или завершая сеансы пользователя. Эти решения можно использовать для управления сетевым трафиком в соответствии с определенными политиками безопасности;
- *Аналитика поведения пользователей (UBA).* Решения UBA собирают информацию о действиях пользователей и сопоставляют их поведение с базовыми показателями. Затем решения используют этот

базовый показатель для сравнения с новым поведением для выявления несоответствий, которые помечаются как потенциальные угрозы [13];

- *Кибербезопасность блокчейна* - это технология, основанная на неизменяемых транзакционных событиях. В технологиях блокчейн распределенные сети пользователей проверяют подлинность транзакций и обеспечивают сохранение целостности [1]. Хотя эти технологии еще не получили широкого распространения, некоторые компании начинают включать блокчейн в другие решения;
- *Обнаружение конечной точки и ответ (EDR).* EDR-решения позволяют отслеживать активность конечных точек, выявлять подозрительную активность и автоматически реагировать на угрозы. Эти решения предназначены для улучшения видимости оконечных устройств и могут использоваться для предотвращения проникновения угроз в сети или утечки информации. Решения EDR полагаются на непрерывный сбор данных о конечных точках, механизмах обнаружения и регистрации событий;
- *Управление состоянием безопасности облака (CSPM)* - это набор методов и технологий, которые можно использовать для оценки безопасности облачных ресурсов. Эти технологии позволяют сканировать конфигурации, сравнивать средства защиты с тестами и обеспечивать единообразное применение политик безопасности. Часто решения CSPM содержат рекомендации или руководства по исправлению ошибок, которые можно использовать для улучшения состояния безопасности.

Данный комплекс мер охватывает всю среду киберпространства, обеспечивая безопасность в сети, в облаке, внутри системы и в других информационных ресурсах, которые чаще всего используются для обмена информацией. Такая стратегия работает на трех уровнях безопасности: мониторинг, обнаружение и устранение угроз, что позволяет эффективно предотвращать компьютерные атаки, несанкционированный доступ, кражу данных и внедрению в систему вредоносных программ.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

## Заключение

Цифровизация – это один из глобальных трендов современной эпохи [15]. С развитием информационного общества мы всё чаще стали сталкиваться с проблемой информационной безопасности [16]. Так как информация стала самым ценным ресурсом, ей необходимо обеспечить надежную защиту, это позволит сохранить конфиденциальность секретных данных пользователей, организаций и государственных структур.

Защита сведений, содержащих государственную тайну и личную информацию граждан, регулируется законодательством Российской Федерации и является обязательной для исполнения. Алгоритмы защиты коммерческой тайны должны устанавливаться самостоятельно, в зависимости от специфики и размера конкретного предприятия или организации. А безопасность личной информации полностью находится в руках самого пользователя, который сам решает, как обезопасить себя и свои данные от рук злоумышленников.

Исследование в рамках данной статьи выявило, что большинство пользователей выстраивает слабую систему защиты, состоящую из самых простых методов, вследствие чего неоднократно подвергаются компьютерным атакам и заражениям вирусами. Такие результаты онлайн-опроса привели к тому, что применение методов защиты отдельно друг от друга не является эффективным способом. Это говорит о том, что пользователям необходимо следовать стратегии информационной безопасности, которая подразумевает использовать полноценный комплекс мер по защите данных. Пример такого комплекса представлен авторами в данной публикации. При дальнейшем исследовании тематики статьи существует возможность расширения и дополнения мер по защите информации. Это связано с тем, что ежедневно компьютерные атаки и

распространение вирусов модернизируются и требуют новые методы их уничтожения и предотвращения.

## Список литературы

1. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны. - ДМК Пресс, 2020. - 327 с.

2. Бабин С.А. Лаборатория хакера. - СПб.: БХВ-Петербург, 2016. - 240 с.

3. Язов Ю.К., Соловьев С.В. Защита информации в информационных системах от несанкционированного доступа. - Воронеж: Кварта, 2015. - 440 с.

4. Скабцов Н. Аудит безопасности информационных систем. - СПб.: Питер, 2018. - 272 с.

5. Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. - 2018. - Т. 10. - № 2. - С. 52-61. - URL: https://elibrary.ru/item.asp?id=34939627 (дата обращения: 28.10.2020).

6. Smith S. The Internet of Risky Things: Trusting the Devices That Surround Us. - O'Reilly Media, 2017. - 240 p.

7. Velu Vijay Kumar. Mobile Application Penetration Testing. - Packt Publishing, 2016. - 312 p.

8. Горлатых А.В., Запечников С.В. Построение защищенной системы управления многомерными структурами данных // Безопасность информационных технологий. - 2018. - Т. 25. - № 3. - С. 16-25. - URL: https://bit.mephi.ru/index.php/bit/article/view/1136 (дата обращения: 19.08.2020).

9. Prakhar P. Mastering Modern Web Penetration Testing. - Packt Publishing, 2016. - 535 p.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

10. Парасрам Ш. и др. Тестирование на проникновение и безопасность. - СПб.: Питер, 2020. - 448 с.

11. Бирюков А.А. Собираем устройства для тестов на проникновение. - М.: ДМК Пресс, 2018. -378 с.

12. Главные тенденции в развитии решений для кибербезопасности // АО «Лаборатория Касперского». - URL: https://www.kaspersky.ru/resource-center/preemptive-safety/cyber-security-trends (дата обращения: 28.10.2020).

13. Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. - 2019. - № 1 (29). - URL: http://cyberrus.com/wp-content/uploads/2019/03/02-09-129- 19_1.-Romashkina.pdf (дата обращения: 25.10.2020).

14. Mueller J.P. Security for Web Developers: Using javascript, HTML, and CSS. - O'Reilly Media, 2015. - 384 p.

15. Самерханова Э.К., Балакин М.А. Подготовка руководителей профессиональных образовательных программ к работе в условиях цифровой среды вуза // Вестник Мининского университета. - 2020. - Т. 8. - № 2. - С. 4. - URL: https://vestnik.mininuniver.ru/jour/article/view/1084/777 (дата обращения: 14.10.2020).

16. Афанасьев С.В. Обоснование актуальности разработки субстратно-атрибутивной модели информационной культуры в рамках философии культуры // Вестник Мининского университета. - . Т. 8. - № 3. - С. 10. - URL: https://vestnik.mininuniver.ru/jour/article/view/1125/800 (дата обращения: 09.10.2020).

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

# Justification of the efficiency of using methods of saving and protecting information of computer systems users

***Ponachugin Alexander Viktorovich***
*Candidate of Economics, associate Professor, Department of Applied Informatics and information technologies in education,*
*Nizhny Novgorod state pedagogical University named after K. Minin*
*sasha3@bk.ru*
***Timofeeva Ksenia Olegovna***
*student, Nizhny Novgorod state pedagogical University named after K. Minin*
*kceni_21_01_99@mail.ru*
***Zaitseva Maria Romanovna***
*student, Nizhny Novgorod state pedagogical University named after K. Minin*
*zaitsevamasha1999@mail.ru*

Types of information, tools and areas used for its protection were considered, and a survey among IT students of NPPU named after Kozma Minin was conducted. In the course of work the following methods were used: theoretical research methods (theoretical analysis and synthesis, abstraction and concretization, study of specialized literature); statistical methods: mathematical processing of data obtained during the survey. Online testing was conducted among future specialists in the field of IT-technologies. The analysis of the results showed that even they face different threats to information security, such as the leakage of confidential information, infection of the system with computer viruses, theft of personal accounts, etc. According to the results of the conducted research and analysis of the received survey results within the limits of this article, what technologies of protection of the information should be used are described. The proposed technologies of protection of important properties of the Internet, such as confidentiality, integrity and availability of protected resources can be used by ordinary Internet users, as well as by organizations, enterprises, large companies, etc. This research can serve as a theoretical basis in forming an idea of actual problems of information security. The proposed set of measures on information protection is aimed at combating the revealed threats, which users most often face. This complex can be used at different enterprises to improve information security.

**Keywords:** security, information, Internet, cybercriminal, protection, threat, vulnerability, cybersecurity.