Доверие и безопасность в информационном обществе

ОБЗОР МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья рекомендована к публикации членом редакционного совета А.А. Стрельцовым 20.12.2021.

Соколова Анна Владимировна

Российский университет транспорта, магистрант
Москва, Российская Федерация
sokolova_ann03@mail.ru

Гришкевич Дарья Дмитриевна

Российский университет транспорта, магистрант
Москва, Российская Федерация
grishkevich.daria@gmail.com

Губенко Инна Михайловна

Кандидат физико-математических наук
Российский университет транспорта, кафедра «Системы управления транспортной инфраструктурой», доцент
Москва, Российская Федерация
img0504@yandex.ru

Аннотация

В работе рассмотрены основные методы и средства защиты персональных данных, подробно разобраны наиболее актуальные из них для пользователя персонального компьютера и интернета. Был произведен анализ наиболее распространенных антивирусных программ. На основании установленных критериев лучшей программой для защиты мобильных устройств оказался Avast Mobile Security.

Ключевые слова

защита персональных данных, защита личной информации, методы защиты информации, средства защиты информации, программные меры защиты персональных данных.

Введение

В настоящее время информационные технологии достигли глобального уровня развития. Большинство людей имеет доступ во всемирную объединенную сеть, а также хранит огромное количество информации на персональных компьютерах, смартфонах, запоминающих устройствах и на облачных сервисах. Ежедневно пользователи публикуют в сети колоссальное количество информации, оставляют персональные данные для пользования различными сайтами или для совершения онлайн-покупок, устанавливают на свои устройства сторонние приложения.

При этом личные данные являются мишенью для злоумышленников, которые стремятся любым способом заполучить их для использования в собственных корыстных целях. Кибератака (хакерская атака) – это вредоносное вмешательство в информационную систему компании, взлом сайтов и приложений, личных аккаунтов и устройств [7]. При успешно реализованной атаке минимальным риском будет неправомерная передача контактной информации пользователя компаниям, которые начнут преследовать их обладателя рекламными объявлениями. Наибольший ущерб связан с заполучением или вымоганием денежных средств. Хакеры могут нанести вред персональным устройствам других пользователей, зашифровать или уничтожить нужную информацию, компрометировать и шантажировать жертву с помощью полученных файлов, украсть банковскую информацию и завладеть чужими денежными средствами, воспользоваться

https://doi.org/10.52605/16059921_2022_03_90

чужими разработками, разгласить конфиденциальные сведения, вмешаться в личную жизнь, действовать в сети от лица других пользователей, что может нанести вред репутации, и т.д. Ущерб от таких атак может быть огромен. Например, в марте 2020 года произошла утечка данных более 267 млн пользователей Facebook. В августе 2020 года в сети были обнаружены персональные данные 150 млн пользователей Facebook, Instagram и LinkedIn [2]. Именно поэтому крайне важно применять методы защиты персональных данных и как можно более надежно оберегать свою личную информацию.

Чаще всего под угрозу попадают данные банковских карт, логины и пароли, информация со смартфонов (заметки, данные о местоположении, просматриваемая на экране информация), документы (паспорта, PDF-файлы с билетами, документы, представляющие коммерческую тайну, и прочая конфиденциальная информация). Согласно исследованию актуальных киберугроз по итогам 2020 года, проведенному компанией Positive Technologies, среди украденных данных частных лиц 36% составляют учетные данные, по 19% приходится на персональные данные и данные платежных карт, 12% – на личную переписку, 14% составляет другая информация [4].

Угрозы безопасности персональных данных могут быть связаны с техническими каналами утечки (утечка речевой и видовой информации, побочные электромагнитные излучения и наводки) и с несанкционированным доступом (применение программных средств операционной системы, специализированное программное обеспечение, вредоносные программы).

Защита информации – это действия, направленные на предотвращение утечки защищаемой информации, а также на предупреждение несанкционированного и непреднамеренного воздействия на защищаемую информацию [1]. Чтобы не попасться на уловки злоумышленников и обезопасить свои данные, необходимо соблюдать ряд мер по защите персональных данных.

Таким образом, целью данной работы является рассмотрение существующих методов и средств зашиты информации, а также практического применения тех из них, которые наиболее актуальны для обычного пользователя.

1 Методы защиты информации

К методам защиты информации относятся: регламентация, побуждение, принуждение, препятствие, маскировка, управление доступом [6].

Регламентация – метод защиты информации путем создания комплекса мероприятий, создающих такие условия обработки, хранения и передачи защищаемой информации, которые минимизируют вероятность успешной реализации атак злоумышленников и несанкционированного доступа.

Побуждение – метод защиты информации путем создания условий, которые сподвигают пользователей соблюдать правила и процедуры работы с информацией по психологическим или морально-этическим соображениям.

Принуждение – метод защиты информации путем создания условий, которые вынуждают пользователей и технических специалистов соблюдать правила и процедуры работы с информацией под угрозой материальной, административной или уголовной ответственности.

Препятствие – метод защиты информации путем создания на пути угрозы к защищаемой информации физической преграды, преодоление которой связано с наличием сложностей для злоумышленника.

Маскировка – метод защиты информации путем преобразования информации в недоступный для злоумышленника вид. Частным примером маскировки является применение криптографических методов защиты. Этот метод представляет собой единственный надежный способ передачи информации по каналам связи большой протяженности.

Управление доступом – метод защиты информации путем регулирования использования всех ресурсов компьютерной информационной системы, таких как базы данных, программное и аппаратное обеспечение. Данный метод включает в себя следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов системы – присвоение персонального уникального признака каждому субъекту или объекту доступа, который однозначно идентифицирует этот субъект или объект в информационной системе;

- аутентификацию объекта или субъекта по представленному им идентификатору – действия по проверке подлинности субъекта или объекта доступа, а также по проверке принадлежности предъявленного идентификатора субъекту или объекту доступа;
- проверку полномочий – контроль соответствия дня недели и времени суток обращения, запрашиваемых ресурсов и процедур установленным в соответствии с регламентом;
- проверка наличия прав на работу и создания условий работы в установленном регламентом порядке;
- протоколирование и регистрация обращений к защищаемым ресурсам – ведение журнала обращений к системе;
- принятие мер при попытках несанкционированного доступа – реагирование на попытку доступа при неподтвержденных полномочиях: сигнализация, отказ в запросе, завершение сеанса и отключение пользователя.

Если говорить о наиболее эффективном методе обезопасить личные данные для обычного пользователя, то им является маскировка, а именно способ криптографической защиты ценной информации с помощью специализированных программ. Например, пользователи персональных компьютеров с Windows могут использовать средство безопасности для шифрования томов BitLocker Drive Encryption, которое является частью операционной системы. На компьютерах с macOS имеется встроенная система полнодискового шифрования FileVault2. Пользователям компьютеров с Linux можно применить систему Linux Unified Key Setup (LUKS)/dm-crypt для шифрования жестких дисков и утилиту Cryptsetup, которая позволяет шифровать также и внешние накопители. Кроссплатформенное программное обеспечение VeraCrypt поддерживает операционные системы Windows, macOS и Linux и позволяет шифровать системные диски, отдельные внутренние и внешние диски. Подобные средства помогают предотвратить несанкционированный доступ к данным за счет усиления защиты файлов и системы.

Использование паролей для персональных компьютеров, смартфонов и приложений также помогает повысить уровень безопасности данных [8].

2 Средства защиты информации

Безопасность информации обеспечивается комплексным применением методов и средств защиты. Методы и средства защиты информации в обобщенном виде представлены на схеме (рис. 1).

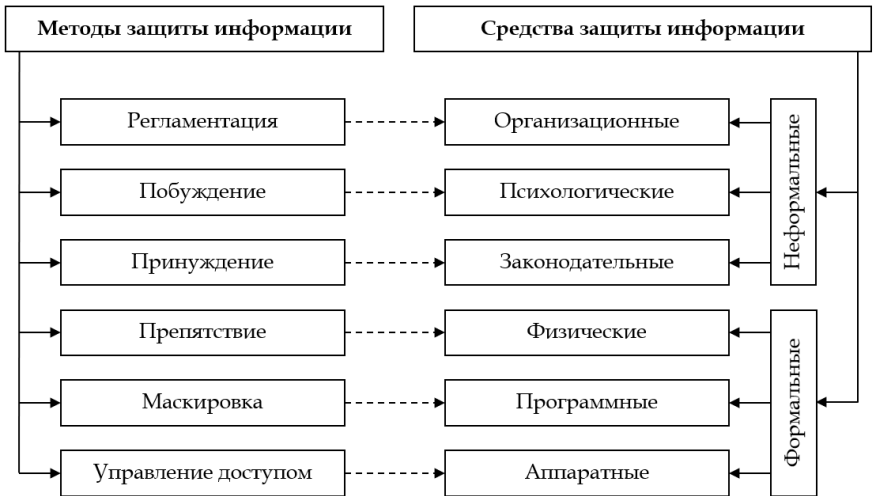

Рис. 1. Методы и средства защиты информации [6]

Средства защиты информации классифицируются на неформальные и формальные [6].

Неформальные (нормативные) средства защиты представляют собой определенные правила, порядки, нормативно-правовые акты и организационные меры, которые связаны с целенаправленной деятельностью человека и регулируют ее. К неформальным средствам защиты информации относятся организационные, законодательные и психологические средства.

Организационные средства защиты реализуются в виде организационно-технических и организационно-правовых мер, которые применяются при создании, тестировании и эксплуатации технических средств, информационных систем, помещений. Данные меры закрепляются в

соответствующем документе, в котором четко фиксируются правила действий технических специалистов и пользователей при работе с вышеназванными объектами. Они позволяют повысить уровень безопасности и минимизировать непреднамеренную утечку информации.

Законодательные средства защиты представлены законодательными актами государства, которые регулируют правила использования, обработки и передачи защищаемой информации. Законодательные акты также предусматривают меры ответственности за нарушение правил обращения с информацией.

Психологические (морально-этические) средства защиты определяются различными традиционно сложившимися принципами, а также нормами, которые формируются с распространением информационных технологий и коммуникаций. Данные принципы и нормы способствуют формированию определенного мышления у людей, при котором они осознают важность обеспечения информационной безопасности и правильного обращения с информацией. Их соблюдение не является обязательным, как, например, соблюдение законодательных норм, но их нарушение может привести к уменьшению авторитета и потере деловой репутации.

Формальные средства защиты выполняются в соответствии с заранее строго определенной процедурой без прямого человеческого вмешательства. К формальным относятся физические, программные, аппаратные средства защиты.

Физические средства защиты осуществляется за счет установки автономных охранных устройств и систем, создающие физические препятствия на пути злоумышленников. Примером физических средств защиты являются надежные двери, запирающие устройства, оконные решетки, сейфы, прочные огнеупорные несущие конструкции помещений, охранная сигнализация.

Программные средства защиты представляют собой специализированное программное обеспечение, используемое для повышения безопасности технических устройств, предотвращения попыток несанкционированного доступа к информации.

Аппаратные средства защиты – это оборудование, которое встраивается или сопрягается с техническими устройствами обработки данных. Аппаратные средства затрудняют несанкционированный съем информации, позволяют обнаруживать потенциальные каналы утечки информации, обеспечивают защиту от системных сбоев.

3 Программные средства защиты на практике

Программные средства защиты персональных данных являются наиболее применимыми и доступными для обычных пользователей. Рассмотрим их более подробно. К программным средствам защиты относятся: встроенные средства защиты, программы для предотвращения несанкционированного доступа, межсетевые экраны, программы диагностики компьютера, антивирусные программы, прокси-серверы, виртуальные частные сети [3] (рис. 2).

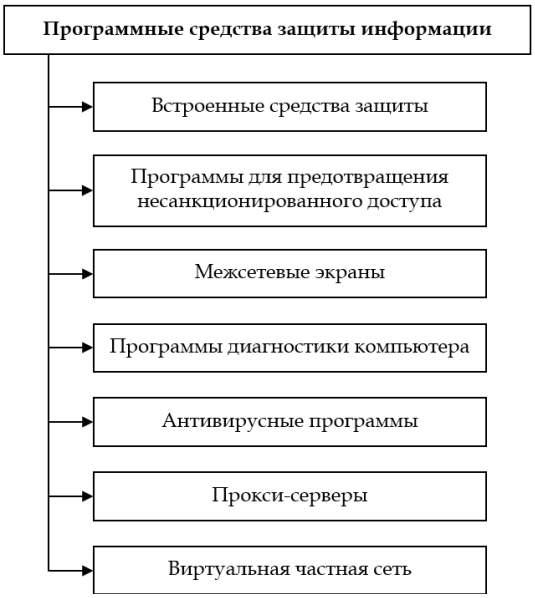

Рис. 2. Программные средства защиты информации

Встроенные средства защиты закрывают информацию от копирования, выполняют идентификацию и авторизацию пользователя, т.е. позволяют войти в систему и совершать определенные действия после ввода корректной комбинации логина и пароля, определяют соответствующие права доступа. Данные средства включают в себя инструменты операционной системы, перераспределяющие порядок выполнения процедур в соответствии с привилегиями или пользовательским режимом, чтобы защитить программы от нежелательного воздействия друг на друга в многопрограммном режиме (когда несколько приложений выполняются параллельно в памяти технического устройства) во избежание сбоев и ошибок в работе каждой из программ и операционной системы.

Программы для предотвращения несанкционированного доступа имеют более широкие возможности, чем встроенные средства защиты. Они могут решать следующие задачи: защита папок и файлов на персональном компьютере, контроль за соблюдением пользователями правил безопасности во время работы, обнаружение и пресечение попыток несанкционированного доступа к защищаемой информации, отслеживание выполняемых на управляемом компьютере действий при автономной работе или в локальной сети.

Межсетевые экраны осуществляют контроль и фильтрацию проходящего через них трафика между глобальной и локальной сетями согласно заданным правилам. Данная технология позволяет практически полностью нейтрализовать опасность несанкционированного вторжения в локальные сети, хотя такой риск все же остается. Более современным способом защиты аналогичной направленности является маскарад, при котором весь исходящий трафик локальной сети отправляется от имени сервера межсетевого экрана, делая локальную сеть необнаружимой.

Программы диагностики компьютера выявляют и предотвращают неполадки и ошибки в работе персонального компьютера и обеспечивают надежную работу программного обеспечения. Инструменты регулярной автоматической проверки системы и средства обеспечения действий по выявлению и устранению ошибок разработки, проектирования и обслуживания уменьшают уязвимости программного обеспечения.

Антивирусные программы выполняют функции обнаружения вирусов, лечения или удаления зараженных файлов и предотвращения воздействия вредоносных программ на данные или операционную систему.

Согласно исследованию 35 антивирусных программ (25 для операционной системы Windows и 10 – для macOS), проведенному Роскачеством и Ассамблеей организаций потребительских испытаний, в пятерку лучших антивирусов 2019 года для операционной системы Windows вошли Bitdefender Internet, ESET Internet, Bitdefender Antivirus Free Edition, Norton Security Deluxe, Avast Free Antivirus, а в тройку лучших антивирусов для операционной системы macOS вошли ESET Cyber Security Pro, Kaspersky Internet Security, Bitdefender Antivirus for Mac [5].

Данный рейтинг может служить помощником при выборе антивирусной защиты для персонального компьютера. На рынке антивирусных программ представлены надежные продукты других компаний, поэтому пользователь может самостоятельно выбрать подходящий вариант, исходя из собственных потребностей, бюджета, предлагаемых возможностей и функций.

Прокси-серверы позволяют передавать исходящие и входящие запросы не напрямую между локальной и глобальной сетями, а через промежуточные серверы-посредники. В результате несанкционированный доступ из глобальной сети в локальную закрывается. Примеры прокси-серверов: CoolProxy (для Windows), ICS (для Linux), 3proxy (кроссплатформенный).

Виртуальная частная сеть (Virtual Private Network – VPN) применяется для безопасной и конфиденциальной передачи информации, которую необходимо защитить от несанкционированной записи или прослушивания. При использовании VPN-программ устройство не напрямую подключается к сайтам, а через зашифрованный канал связи соединяется с частной виртуальной сетью. И уже эта сеть подключается к нужному сайту и передает пользователю информацию. Таким образом, сайты получают информацию не о реальном пользователе, а о случайном IP-адресе из частной виртуальной сети.

Маловероятно, что злоумышленники будут отслеживать пользователей, выходящих в интернет с домашнего компьютера, и совершать попытки кражи их информации. Но при выходе в сеть в общественных местах соединение будет уязвимо и вероятность утечки информации или взлома сильно возрастает. Использование виртуальной частной сети снизит данные риски.

Известными надежными сервисами VPN являются Surfshark, IPVanish, NordVPN, Cyberghost, ExpressVPN. Все они могут быть использованы на персональных компьютерах с операционной системой Windows и macOS.

4 Анализ антивирусных программ для мобильных устройств

На сегодняшний день все больше информации пользователи хранят на мобильных устройствах. Проведем сравнительный анализ трех наиболее популярных бесплатных программ-антивирусов для смартфонов (на основе рейтинга Play Market): Kaspersky Mobile Antivirus; Dr.Web Light; Avast Mobile Security.

Выделим критерии для сравнения функций антивирусных программ: защита в реальном времени, проверка по запросу пользователя, проверка по расписанию, проверка отдельных файлов и папок, проверка архивов, проверка съемных носителей, отслеживание изменений в системной области, обезвреживание, удаление и карантин угроз, встроенный межсетевой экран для блокирования действий злоумышленников, блокировка доступа к опасным сайтам, разблокировка устройства при блокировании программой-вымогателем, поиск и блокировка потерянного устройства, выявление потенциальных рисков конфиденциальности, сканирование точки доступа беспроводных сетей. Результаты анализа представлены в таблице (см. табл. 1).

Таблица 1. Сравнительный анализ антивирусных приложений для мобильных устройств

Критерии \ Антивирус	Kaspersky Mobile Antivirus	Dr.Web Light	Avast Mobile Security
Защита в реальном времени	+	-	+
Проверка по запросу пользователя	+	+	+
Проверка по расписанию	-	+	+
Проверка отдельных файлов и папок	+	+	+
Проверка архивов	+	+	+
Проверка съемных носителей	+	-	-
Отслеживание изменений в системной области	+	-	-
Обезвреживание, удаление и карантин угроз	+	+	+
Встроенный межсетевой экран для блокирования действий злоумышленников	-	-	+
Блокировка доступа к опасным сайтам	-	+	+
Разблокировка устройства при блокировании программой-вымогателем	+	-	-
Поиск и блокировка потерянного устройства	-	+	+
Выявление потенциальных рисков конфиденциальности	+	-	+
Сканирование точки доступа беспроводных сетей	-	-	+

Все антивирусные программы включают в себя фиксированный набор компонентов безопасности: активация проверки устройства пользователем, проверка файлов и папок различного типа и принятие мер при обнаружении угроз.

Из приведенного анализа можно сделать вывод, что в настоящее время наилучшим мобильным антивирусным приложением по выбранным критериям является Avast Mobile Security.

Заключение

В работе продемонстрированы основные методы и средства защиты персональных данных, подробно разобраны наиболее актуальные из них для пользователя персонального компьютера и интернета.

На основании проведенного сравнительного анализа наиболее распространенных антивирусных программ по 14 критериям лучшей программой для защиты мобильных устройств оказалась Avast Mobile Security.

Защита личной информации является важной задачей каждого пользователя, ведь ежедневно злоумышленники совершают попытки хищения персональных данных, ущерб от несанкционированного использования которых может быть значителен. Исправление негативных последствия от успешно реализованной атаки может потребовать больших ресурсов или быть невозможным, поэтому крайне необходимо принимать предупреждающие меры и надежно защищать собственную информацию.

Литература

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. URL: https://docs.cntd.ru/document/1200058320 (дата обращения: 10.12.2021).
2. Десять самых громких кибератак XXI века. URL: https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e (дата обращения: 10.12.2021).
3. Информационные технологии в экономике и управлении в 2 ч. Часть 1: учебник для вузов / В.В. Трофимов [и др.]; под редакцией В.В. Трофимова. – 3-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2021. 269 с.
4. Исследование актуальных киберугроз Positive Tehnologies: итоги 2020 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/#id1 (дата обращения: 10.12.2021).
5. Исследование антивирусов Роскачество совместно с Международной ассамблеей организаций потребительских испытаний для операционной системы Windows и macOS. URL: https://rskrf.ru/ratings/tekhnologii/programmnoe-obespechenie/antivirusy (дата обращения: 10.12.2021).
6. Коноплева, И.А. Информационные технологии: учебное пособие / И.А. Коноплева, О.А. Хохлова, А.В. Денисов. – 2-е изд. – Москва: Издательство «Проспект», 2014. 275 с.
7. Определение кибератаки. URL: https://www.cisco.com/c/ru_ru/products/security/common-cyberattacks.html (дата обращения: 10.12.2021).
8. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства: учебное пособие. – Саратов: Издательство «Профобразование», 2017. 544 с.

OVERVIEW OF METHODS AND MEANS OF PROTECTING PERSONAL DATA

Sokolova, Anna Vladimirovna

Russian University of Transport, undergraduate student
Moscow, Russian Federation
sokolova_ann03@mail.ru

Grishkevich, Daria Dmitrievna

Russian University of Transport, undergraduate student
Moscow, Russian Federation
grishkevich.daria@gmail.com

Gubenko, Inna Mikhailovna

Candidate of physical and mathematical sciences
Russian University of Transport, Department of Transport Infrastructure Management Systems, associate professor
Moscow, Russian Federation
img0504@yandex.ru

Abstract

The paper discusses the main methods and means of protecting personal data, the most relevant of them for a user of a personal computer and the Internet are analyzed in detail. The analysis of the most common anti-virus programs was carried out. Based on the established criteria, Avast Mobile Security was the best program for protecting mobile devices.

Keywords

protection of personal data, protection of personal information, methods of protecting information, means of protecting information, software measures for protecting personal data.

References

1. GOST R 50922-2006. Zashchita informacii. Osnovnye terminy i opredeleniya. URL: https://docs.cntd.ru/document/1200058320 (accessed: 10.12.2021).
2. Desyat' samyh gromkih kiberatak XXI veka. URL: https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e (accessed: 10.12.2021).
3. Informacionnye tekhnologii v ekonomike i upravlenii v 2 ch. CHast' 1: uchebnik dlya vuzov / V.V. Trofimov [i dr.]; pod redakciej V.V. Trofimova. – 3-e izd., pererab. i dop. – Moskva: Izdatel'stvo YUrajt, 2021. 269 s.
4. Issledovanie aktual'nyh kiberugroz Positive Tehnologies: itogi 2020 goda. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/#id1 (accessed: 10.12.2021).
5. Issledovanie antivirusov Roskachestvo sovmestno s Mezhdunarodnoj assambleej organizacij potrebitel'skih ispytanij dlya operacionnoj sistemy Windows i macOS. URL: https://rskrf.ru/ratings/tekhnologii/programmnoe-obespechenie/antivirusy (accessed: 10.12.2021).
6. Konopleva, I.A. Informacionnye tekhnologii: uchebnoe posobie / I.A. Konopleva, O.A. Hohlova, A.V. Denisov. – 2-e izd. – Moskva: Izdatel'stvo «Prospekt», 2014. 275 s.
7. Opredelenie kiberataki. URL: https://www.cisco.com/c/ru_ru/products/security/common-cyberattacks.html (accessed: 10.12.2021).
8. SHan'gin, V.F. Zashchita komp'yuternoj informacii. Effektivnye metody i sredstva: uchebnoe posobie. – Saratov: Izdatel'stvo «Profobrazovanie», 2017. 544 s.