Шумилина В.Е., доцент кафедры «Экономическая безопасность, учет и право» ФГБОУ ВО «Донской государственный технический университет», Ростов-на-Дону, Россия;
Голубова А.Г.,студент 3 курса кафедры «Экономическая безопасность, учет и права» ДГТУ, Ростов – на – Дону, Россия;

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ В СОВРЕМЕННОМ ОБЩЕСТВЕ

Аннотация. Данная статья рассматривает принципы информационной безопасности, способы, которые помогают обеспечить защиту информации. Рассматриваются проблемы защиты информации, несанкционированного доступа к ней. Демонстрирует виды вирусов, которые существуют в Интернете. Предлагается программное обеспечение, которое поможет пользователю защитить себя от них.

Ключевые слова: информационная безопасность, информация, защита информации, антивирус, информационные технологии, безопасность информации.

Shumilina V. E., associate Professor of «Economic safety, accounting and Law» of the «Donskoy state technical University», Rostov-on-Don, Russia;
Golubova A.G.,student of the Department of «Economic Security, Accounting and Law» DGTU, Rostov-on-Don, Russia;

INFORMATION SECURITY AND DATA PROTECTION IN MODERN SOCIETY

Annotation. This article looks at the principles of information security, and the ways in which information can be protected. Examines the problems of protecting information, unauthorised access to it. Demonstrates the types of viruses that exist on the Internet. Offers software to help the user protect themselves from them.

Keywords: information security, information, information protection, antivirus, information technology, information security.

Информационные технологии стремительно развиваются. Из-за этой особенности они легко и быстро влились в быт человека. На сегодняшний момент человек не может представить свое существование без:

- социальных сетей;
- онлайн магазинов;

- бесконечного количества мессенджеров;

- банков-онлайн и многого другого.

Именно поэтому безопасность информации в интернет пространстве является актуальной проблемой в наше время. Из-за бурного роста технологий, скрывать личную информацию, иметь конфиденциальность становится все сложнее.

Самой распространенной информационной «дырой» является безопасность, во время пользования мобильными банковскими приложениями. Клиенты банков общаются с ним посредством следующих способов:

-банк-клиент или онлайн-банкинг через персональные компьютеры;

- онлайн приложения в мобильном устройстве;

- социальные сети и популярные мессенджеры.

Согласно результатам исследований, проведенного аналитического центра НАФИ, в 2020 году в России 56% граждан пользуются цифровыми каналами управления личными финансами - мобильным приложением или интернет-банком.

Более 10 лет в сети ходят анекдоты про искусственный интеллект, который от имени банка дает советы детям. Популярный сегодня маркетинговый тренд «smartdata» предполагает максимально персонифицированный сбор данных о клиенте, где на основе одного распространенного поля-индикатора можно получить комплексный портрет клиента. Именно здесь вступает роль информационная безопасность. Пользователь интернета, зачастую, не задумываясь подписывается на рассылку любой информации, которая носит в себе рекламный характер, регистрируется на различном количестве сайтов под одним и тем же псевдонимом (логин). Именно это помогает верифицировать вас, как клиента, и собирать при этом вашу личную информацию, использовать ее в своих целях. Такое может произойти, например, при приеме на работу. Потенциальный работодатель анализирует ваш профиль в социальных сетях.

Так же отмечают случаи контекстной рекламы, которые возникают на основе вашего поиска в интернете за определенное количества времени. Они отмечают ваши предпочтения, интересы, идентифицируют вас, как клиента, и начинают предлагать рекламу соответствующего характера.

Именно из-за этого персональные данные пользователей и их информационная безопасность требует тщательного разбора и внимания. В соответствии с Законом о безопасности и содержанием Концепции национальной безопасности РФ под информационной безопасностью будем понимать состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере.

Безопасность информации – это состояние защищенности данных, при которых обеспечены их доступность, конфиденциальность и безопасность от внутренних и внешних угроз. То есть информация должна быть:

- защищена от взлома извне;

- недоступна для неуполномоченных лиц.

Защита информации — это комплекс мероприятий, направленных на обеспечение информационной безопасности. Зачастую, крупные кампании и организации создают собственные системы информационной безопасности для минимизации шансов утечки данных. Такая информация касается финансовой отчетности организации, ее деятельности, личные данные о персонале. Для реализации мерз защиты необходимо проводить организационные мероприятия для персонала, назначать ответственных лиц за информационную безопасность, введение дополнительных правил и инструкций пользования сетью на рабочем месте, установление дополнительных программных обеспечений для безопасности информации. Современные организации используют международные рекомендации для построения систем управления безопасностью и использует лучшие мировые практики.Согласно статистике объем российского рынка информационной безопасности (ИБ) по итогам 2021 года достиг 98,6 млрд рублей,

увеличившись на 8% в сравнении с 2020-м. Об этом свидетельствуют данные компании «Ростелеком-Солар», раскрытые 23 декабря 2021 года.

В компании «Информзащита» согласились с 8-процентным ростом рынка, но назвали другой показатель в денежном выражении — 81,5 млрд рублей. Некоторые организации заявляют, что такие показатели являются «пессимистскими», т.к. по их проведенным исследованиям рост рынка информационной безопасности составил от 10% и более. Уровень спроса на информационную безопасность остается примерно таким же, как это было в 2020 году. Ожидается планомерный рост рынка информационной безопасности.

Компании переходят на новый технологический уровень, что также оказывает влияние на требования к информационной безопасности.

По мнению Анны Кирсановой, начальника отдела маркетинга компании "Гарда Технологии", технологический уровень экономикообразующих предприятий в целом растет небывалыми темпами, что подстегивает и развитие рынка ИБ как сопутствующей инфраструктуры.

Любую информацию необходимо охранять, внезависимости от того, каким образом она хранится или используется. В наше время существует большое количество информационных проблем, поэтому грамотный руководитель должен оценивать состояние собственной информационной сети. Для этого руководитель организации может проводить повышение квалификации ответственных лиц и пользователей, которые работают с важной информацией, основам и особенностям информационной безопасности. В дополнение к этому устанавливаются и регулярно обновляются антивирусные защитные программы, производится шифрование данных.

Необходимо использовать дополнительные меры защиты данных организации. Проводится модернизация, ремонт уже существующей локальной сети, устанавливается дополнительное оборудование – видеокамеры, сигнализации, резервные серверы, источники альтернативного

питания и многое другое. Данные методы защиты помогут организации избежать утечки важных данных, обеспечить бесперебойную работу информационной системе в случае хакерских атак.

Важной частью данного вопроса является сооружение личной безопасности данных. Поскольку нынешнее поколение способно быстро освоить новые технологии, разобраться и усвоить правила их пользования, возникает проблема с оценкой реальных рисков, которые могут возникнуть при работе с Интернетом. Зачастую, только после поломки или утери важной информации для пользователя, начинаешь задумываться над тем, чтобы улучшить или модернизировать собственную информационную безопасность.

В быту защита личных данных касается исключительно от вирусов или вирусных программ, которые легко можно зацепить в сети Интернет. Компьютерный вирус — вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи. Данное название подобрано не случайно. Данный код представляет собой биологический вирус. Он имеет собственные виды:

- черви;
- троянские программы (Троян);
- полиморфные вирусы и другое.

Как известно: если существует вирус, то должен быть и антивирус. В нашем случае здесь все прозрачно, защитное программное обеспечение для компьютеров – антивирус. Это специализированная программа, предназначенная для выявления, предотвращения обнаружения компьютерных вирусов. Также одной из функций антивируса является восстановление зараженных файлов вирусами.

Данная программа является лишь вспомогательным инструментом, которая поможет ее пользователю не потерять свои личные данные. Основная функция защиты лежит на самом человеке. Необходимо

нивелировать риски и угрозы, на которые нельзя закрывать глаза. Пользуясь сетью Интернет, не рекомендуется использовать пароли:

- простые;
- короткие (не менее 8 знаков);
- однотипные.

Он должен быть разнообразным, содержать в себе набор и букв, и цифр, которые будут обеспечивать защиту ваших данных. Еще одним способом лично защитить самостоятельно свои данные является установка антивируса. В настоящее время на просторе Интернета существует много версий данной программы, которые имеют свои плюсы и минусы. Из-за этого следует обратиться к специалисту, который сможет вам посоветовать надежный антивирус, объяснит, как его правильно установить и использовать в дальнейшем.

Человеку, который решил выйти в сеть Интернет в качестве пользователя, работать в нем, необходимо освоить его, изучить. Самый главный враг для вашего компьютера – сам пользователь. Периодически могут возникать баннеры, носящие в себе сообщения рекламного характера, которые будут переадресовывать вас на сомнительные сайты. Благодаря собранной информации, мы знаем, что антивирус нас может спасти от той участи, когда пользователь переходит по ссылке на сайт и рискует потерять все свои данные. Как в жизни, так и в Интернете, необходимо использовать надежные ссылки и сайты для обеспечения безопасности вашей личной информации.

Необходимо помнить и о безопасности вашей личной информации, которую ни в коем случае не стоит размещать в интернете, если вы не убеждены в том, что сайт является надежным источником хранения данных:

- имени, фамилии;
- номера телефона;
- города проживания;
- адреса проживания;

- номера кредитной карты;

- паспортных данных и т.д.

Благодаря данным способам, любой пользователь может обеспечить личную информационную безопасность. Это снижает риски несанкционированного доступа к информации.

Таким образом, пользователю платформы Интернет необходимо всегда обновлять свои знания о том, как пользоваться компьютером, какие существуют средства защиты информации в Интернете и как дополнительно можно обезопасить свои конфиденциальные данные. Информационная безопасность в наше время – ключевой способ защитить свою важную или потенциально полезную информацию от несанкционированного доступа.

Литература

1. Белов Е. Б., Лось В. П. Основы информационной безопасности. М.: Горячая линия: Телеком, 2016.
2. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации. 3-е изд. М.: Академия, 2018.
3. Шумилина, В. Е. Информационные технологии и медиатизация общества / В. Е. Шумилина, Д. А. Лагутин // Экономика России: проблемы, тенденции, прогнозы : Сборник статей по материалам международной научно-практической конференции, Мельбурн, 29 декабря 2021 года. – Мельбурн: AUSPUBLISHERS, 2021. – С. 98-106. – DOI 10.26526/conferencearticle_61cc296c2f4e38.40497971. – EDN UHCLNQ.
4. Шумилина, В. Е. Информационная безопасность как составляющая экономической безопасности предприятия / В. Е. Шумилина, Е. В. Тетунашвили // Управление безопасностью

бизнеса в современных условиях. – Москва : AUSPUBLISHERS, 2021. – С. 119-129. – EDN FESZVK.

5. Шумилина, В. Е. Цифровизация экономики России на современном этапе / В. Е. Шумилина, Д. В. Климов // Экономика государств и территорий: мировые тенденции и проблемы. – Мельбурн : AUS PUBLISHERS, 2021. – С. 104-118. – EDN MMKVRQ.
6. Шумилина, В. Е. Управление информационными рисками в организации / В. Е. Шумилина, О. В. Асташова, А. А. Аистова // Наука и мир. – 2021. – № 1. – С. 36-40. – DOI 10.26526/2307-9401-2021-1-36-40. – EDN ZLBFQA.

References

1. Belov E. B., Los V. P. Fundamentals of information security. M.: Hotline: Telecom, 2016.

2. Melnikov V. P., Kleymenov S. A., Petrakov A. M. Information security and information protection. 3rd ed. M.: Academy, 2018.

3. Shumilina, V. E. Information technologies and mediatization of society / V. E. Shumilina, D. A. Lagutin // Economy of Russia: problems, trends, forecasts: Collection of articles based on materials of the international scientific and practical conference, Melbourne, December 29 2021. - Melbourne: AUSPUBLISHERS, 2021. - P. 98-106. – DOI 10.26526/conferencearticle_61cc296c2f4e38.40497971. – EDN UHCLNQ.

4. Shumilina, V. E. Information security as a component of the economic security of an enterprise / V. E. Shumilina, E. V. Tetunashvili // Management of business security in modern conditions. - Moscow: AUSPUBLISHERS, 2021. - P. 119-129. – EDN FESZVK.

5. Shumilina, V. E. Digitalization of the Russian economy at the present stage / V. E. Shumilina, D. V. Klimov // Economy of States and Territories: World

Trends and Problems. - Melbourne : AUS PUBLISHERS, 2021. - P. 104-118. – EDN MMKVRQ.

6. Shumilina, V. E. Management of information risks in an organization / V. E. Shumilina, O. V. Astashova, A. A. Aistova // Science and World. - 2021. - No. 1. - P. 36-40. – DOI 10.26526/2307-9401-2021-1-36-40. – EDN ZLBFQA.