УДК 33 **DOI: 10.34670/AR.2021.11.42.018**

Информационная безопасность: современные реалии

Ершова Елизавета Евгеньевна

Независимый исследователь,
119019, Российская Федерация, Москва, ул. Воздвиженка, 3/5;
e-mail: infinity609@mail.ru

Бойко Валерий Леонидович

Кандидат экономических наук, доцент,
доцент кафедры экономической безопасности,
Институт права и национальной безопасности,
Российская академия народного хозяйства и государственной службы
при Президенте РФ,
119571, Российская Федерация, Москва, просп. Вернадского, 84;
e-mail: boyko-vl@ranepa.ru

Аннотация

Человеческое общество сегодня уже невозможно представить без современных средств для работы с информацией и ее обработки. Широкие возможности, которые предоставляют цифровые электронные средства, предопределили их массовое распространение. Как следствие, уже в конце 70-х годов XX века появились публикации, где говорилось про возможность радиотехнического канала утечки информации, которую обрабатывали с помощью средств цифровой техники. Но с течением времени данная проблема не решилась, а наоборот, стала еще более острой. Информационной безопасности сегодня отводится крайне важная роль в человеческой жизни, поскольку с развитием технологий становится все сложнее защищать личные данные. Пути решения данного вопроса требуют детального рассмотрения. Информационная безопасность – это предотвращение несанкционированного доступа, использования, искажения, изменения, исследования, записи или уничтожения информации, данных, ресурсов, систем и т.д. Безопасность информации – это состояние защищенности данных, при котором обеспечены их доступность, конфиденциальность и целостность. Под доступностью данных подразумевают их свойство, которое определяет возможность их получить и использовать в дальнейшем по требованию уполномоченных лиц, под конфиденциальностью – свойство, связанное с тем, что такие данные не станут доступны для третьих лиц без согласия уполномоченных лиц, а под целостностью – неизменность информации в процессе хранения или передачи.

Для цитирования в научных исследованиях

Ершова Е.Е., Бойко В.Л. Информационная безопасность: современные реалии // Экономика: вчера, сегодня, завтра. 2021. Том 11. № 2А. С. 145-150. DOI: 10.34670/AR. 2021.11.42.018

Ключевые слова
Информация, безопасность, структура, развитие, форма.

Введение

В настоящее время почти каждый человек является активным пользователем сети Интернет. Люди повсеместно пользуются различными социальными сетями, мессенджерами, приложениями для онлайн-покупок, мобильными банками и др. Однако разработчики данных приложений не гарантируют стопроцентную безопасность, а значит данные пользователей могут спокойно попасть к третьим лицам [Босова, Селищев, 2019, 296].

Вместе с тем информация должна быть достаточно защищенной от взлома извне, ее должно оперировать достаточно образованное лицо, она должна быть недоступной для неуполномоченных лиц.

Основная часть

Защита информации – это комплекс мероприятий, направленных на то, чтобы обеспечить информационную безопасность. Многие организации выстраивают собственные системы информационной безопасности, проводят проверки и анализируют защищенность данных. Это касается как персональных данных клиентов и персонала банков и государственных учреждений, так и информации о текущей деятельности и финансовом состоянии каждой современной организации и предприятия.

Реализация мер защиты включает организационные мероприятия: назначаются ответственные за информационную безопасность, разрабатываются правила и инструкции для пользователей, внедряется политика резервного копирования и др. Сейчас фирмы используют требования международных стандартов, чтобы строить системы информационной безопасности, и используют для этого лучшие практики [Грошева, Невмержицкий, 2017, 36].

Вне зависимости от того, как информация сохраняется, каким образом она используется, следует реализовывать адекватные меры по защите. Каждый современный руководитель должен объективно оценивать текущее состояние информационных систем, четко видеть и понимать нужду в информационном обеспечении и существующие информационные проблемы.

Именно для этого в организации нужно проводить обучение ответственных лиц и пользователей определенным моментам работы с данными, в том числе и нормам информационной безопасности. Как следствие, устанавливаются программные средства защиты, программное обеспечение, регулярно обновляются антивирусные программы, шифруются данные и т.д.

Не менее актуальной является и построение личной информационной безопасности пользователей. Использование компьютеров, планшетов, смартфонов сегодня стало неотъемлемой частью жизни каждого человека. Современное поколение с легкостью осваивает информационные технологии и зачастую уделяет недостаточное внимание рискам, возникающим при работе в системе Интернет, использовании съемных носителей информации и т.д. Иногда только потеря информации или внезапно возникшие проблемы с компьютером заставляют понять на необходимость усиления средств защиты и изучения проблемы информационной безопасности.

В быту защита информации в основном рассматривается как защита от вирусных программ, или вирусов. Компьютерный вирус – это вид вредоносного программного обеспечения, который способен создавать свои копии, внедряться в код других программ, загрузочные секторы или системные области памяти, а также распространять «себя» по различным каналам связи. Компьютерный вирус был так назван неспроста: можно сравнить его распространение с биологическим вирусом. У него есть множество видов: Черви, Троянские программы, Полиморфные вирусы и многие другие.

Все эти вирусы действует по-своему, и постоянно появляются все новые вирусы. Однако есть средства противодействия им – антивирусы.

Антивирус – это специализированная программа, которая предназначается для того, чтобы обнаруживать, устранять и предотвращать появление компьютерных вирусов. Также одной из функций антивируса является восстановление зараженных вирусами файлов.

Защитить важную для себя информацию может любой человек. Для этого достаточно не игнорировать существующие угрозы. Так, например, не нужно использовать простые пароли: «0000» на телефоне или «parol» на электронной почте могут привести к потере важных данных. Чтобы пароль был надежен, он должен состоять из букв и цифр, иметь больше 8 знаков, содержать как заглавные, так и прописные буквы, а также не совпадать ни с одним словарным словом. Нужно использовать защиту от них [Кинг, 2014, 291].

На современном рынке существуют множество антивирусов, подобрать простой и эффективный сейчас очень легко. Хотя перед его установкой лучше проконсультироваться со специалистом. Кроме того, установленный антивирус следует периодически обновлять.

В последнее время все чаще проявляются атаки с использованием методов социальной инженерии, какие сами по себе являются более изощренными, и непросто их найти и остановить с помощью систем обнаружения взломов. Методы защиты от подобных атак, постоянно совершенствуясь, включают в себя следующие рекомендации:

– установить самые безопасные почтовые и веб-шлюзы для фильтрации вредоносных ссылок;

– постоянно проводить мониторинг писем и отмечать поступающие из внешней, некорпоративной сети;

– настроить систему оповещения на обнаружение доменных имен, которые похожи на имя компании или организации;

– проводить обучение на постоянной основе сотрудников организации новейшим технологиям социальной инженерии, организуя обучающие семинары с привлечением сотрудников компаний-партнеров; на семинарах рекомендуется применять технологии ролевых игр с делением сотрудников на команды злоумышленников и защиты [Васильев , www];

– разбить корпоративную сеть предприятия на более мелкие элементы и усилить контроль при осуществлении доступа к каждому из них. Полномочия сотрудников сузить до минимально необходимых для выполнения ими рабочих обязанностей. При управлении правами доступа необходимо отталкиваться от принципа нулевого доверия;

– разработать и внедрить процедуры авторизованного внесения внеочередных изменений в систему для обработки срочных запросов руководства и своевременно знакомить с ними сотрудников, которые имеют доступ к конфиденциальной информации;

– ввести многофакторную аутентификацию для защиты ключевых систем и аккаунтов сотрудников, работающих с конфиденциальной информацией;

– настроить контроль аномальной активности в корпоративной сети, например, такой как

медленное копирование данных из системы, копирование данных в нерабочее время, особенно из офисов, где уже не осталось сотрудников в конце рабочего дня, попытки сбора внутренней информации;

– проводить мониторинг аномальных или избыточных LDAP-запросов, которыми активно пользуются злоумышленники с целью изучения структуры сетей разных предприятий;

– ограничить круг доверенных программ для немногозадачных серверов;

– проводить установку последних патчей на всех рабочих станциях; найти и устранить бэкдоры в случае обнаружения атаки;

– осуществлять грамотный риск-менеджмент.

Используя различные способы защиты по максимуму, пользователи создают свою систему информационной безопасности, которая позволит сохранить свои данные, а также снизить до минимума риски несанкционированного доступа к различного рода сведениям, которые имеют важное значение в жизни.

Заключение

Таким образом, используя различные средства защиты информации и придерживаясь определенного ряда правил при работе с компьютером и сетью Интернет, можно сохранить важные данные, а также снизить до минимума возможность несанкционированного доступа к ним.

Можно подытожить, что в вопросе противодействия современным кибератакам и прочим информационным рискам на первом месте находится информированность и время реакции. Поэтому информационная безопасность сегодня – это не состояние, а определенный процесс; причем это процесс, который постоянно требует динамичных изменений и является крайне чувствительным к любым задержкам [Информационная безопасность: построения системы управления, www].

Библиография

1. Ахметьянова А.И., Кузнецова А.Р. Проблемы обеспечения информационной безопасности в России и ее регионах // Фундаментальные исследования. 2016. № 8-1. С. 82-86.
2. Босова Е.Д., Селищев В.А. Информационная безопасность: современные реалии // Известия ТулГУ. Технические науки, 2019. Вып. 9. С. 296-300.
3. Васильев В. Информационная безопасность: исторические аллюзии и современные реалии. URL: https://www.itweek.ru/security/article/detail.php?ID=124939.
4. Галушкин А.А. К вопросу о значении понятий «национальная безопасность», «информационную безопасность», «национальная информационная безопасность» // Правозащитник. 2015. № 2.
5. Грошева Е.К., Невмержицкий П.М. Информационная безопасность: современные реалии // Бизнес-образование в экономике знаний. 2017. № 3. С. 35-38.
6. Информационная безопасность: построения системы управления. URL: https://gpi.kz/wp-content/uploads/2019/02/GPIC_IT-security.pdf.
7. Кинг Б. Банк 3.0. М.: ЗАО «Олимп-Бизнесс», 2014. 474 с.
8. Кривоухов А.А. Информационная безопасность как мера обеспечения национальной безопасности России // Государство и общество: вчера, сегодня, завтра. Серия: Право. 2013. № 9(3).
9. Родичев Ю. Нормативная база и стандарты в области информационной безопасности. СПб.: Юпитер, 2018. 256 с.
10. Спирина С.Г. Информационные технологии оценки финансовой устойчивости предприятий (корпораций) // Информационные ресурсы России. 2015. № 3. С. 22-26.

Information security: modern realities

Elizaveta E. Ershova

Independent Researcher,
119019, 3/5, Vozdvizhenka str., Moscow, Russian Federation;
e-mail: infinity609@mail.ru

Valerii L. Boiko

PhD in Economics, Associate Professor,
Associate Professor of the Department of economic security,
Institute of Law and National Security,
Russian Presidential Academy of National Economy and Public Administration,
119571, 84, Vernadskogo av., Moscow, Russian Federation;
e-mail: boyko-vl@ranepa.ru

Abstract

Human society today is impossible to imagine without modern tools for working with information and its processing. The wide opportunities provided by digital electronic means have predetermined their mass distribution. As a result, in the late 70s of the twentieth century, there were publications that spoke about the possibility of a radio channel for information leakage, which was processed using digital technology. But over time, this problem has not been solved, but, on the contrary, has become even more important, as with the development of technology, it becomes more difficult to protect personal data. Information security today plays an extremely important role in human life, as the development of technology makes it increasingly difficult to protect personal data. Therefore, solutions to this issue require detailed consideration. Information security is the prevention of unauthorized access, use, distortion, modification, research, recording or destruction of information, data, resources, systems, etc. Information security is the state of data security, under which their availability, confidentiality and integrity are ensured. The availability of data means their property, which determines the ability to receive and use them in the future at the request of authorized persons, confidentiality is property, related to the fact that such data will not be available to third parties without the consent of authorized persons, and integrity is the immutability of information in the process of storage or transfer.

For citation

Ershova E.E., Boiko V.L. (2021) Informatsionnaya bezopasnost': sovremennye realii [Information security: modern realities]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 11 (2A), pp. 145-150. DOI: 10.34670/AR.2021.11.42.018

Keywords

Information, security, structure, development, form.

References

1. Akhmet'yanova A.I., Kuznetsova A.R. (2016) Problemy obespecheniya informatsionnoi bezopasnosti v Rossii i ee regionakh [Problems of ensuring information security in Russia and its regions]. *Fundamental'nye issledovaniya*

[Fundamental research], 8-1, pp. 82-86.
2. Bosova E.D., Selishchev V.A. (2019) Informatsionnaya bezopasnost': sovremennye realii [Information security: modern realities]. *Izvestiya TulGU. Tekhnicheskie nauki* [News of Tula State University. Engineering Science], 9, pp. 296-300.
3. Galushkin A.A. (2015) K voprosu o znachenii ponyatii "natsional'naya bezopasnost'", "informatsionnuyu bezopasnost'", "natsional'naya informatsionnaya bezopasnost'" [On the question of the meaning of the concepts "national security", "information security", "national information security"]. *Pravozashchitnik* [Human rights defender], 2.
4. Grosheva E.K., Nevmerzhitskii P.M. (2017) Informatsionnaya bezopasnost': sovremennye realii [Information security: modern realities]. *Biznes-obrazovanie v ekonomike znanii* [Business education in the knowledge economy], 3, pp. 35-38.
5. *Informatsionnaya bezopasnost': postroeniya sistemy upravleniya* [Information security: building a control system]. Available at: https://gpi.kz/wp-content/uploads/2019/02/GPIC_IT-security.pdf [Accessed 16/09/2020].
6. King B. (2014) *Bank 3.0* [Bank 3.0]. Moscow: ZAO "Olimp-Bizness" Publ.
7. Krivoukhov A.A. (2013) Informatsionnaya bezopasnost' kak mera obespecheniya natsional'noi bezopasnosti Rossii [Information security as a measure of ensuring the national security of Russia]. *Gosudarstvo i obshchestvo: vchera, segodnya, zavtra* [State and society: yesterday, today, tomorrow], 9(3).
8. Rodichev Yu. (2018) *Normativnaya baza i standarty v oblasti informatsionnoi bezopasnosti* [Normative base and standards in the field of information security]. Saint Petersburg: Yupiter Publ.
9. Spirina S.G. (2015) Informatsionnye tekhnologii otsenki finansovoi ustoichivosti predpriyatii (korporatsii) [Information technologies for assessing the financial stability of enterprises (corporations)]. *Informatsionnye resursy Rossii* [Information resources of Russia], 3, pp. 22-26.
10. Vasil'ev V. *Informatsionnaya bezopasnost': istoricheskie allyuzii i sovremennye realii* [Information security: historical allusions and modern realities]. Available at: https://www.itweek.ru/security/article/detail.php?ID=124939 [Accessed 16/09/2020].