

УДК 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: СОВРЕМЕННЫЕ ПРОБЛЕМЫ И РЕШЕНИЯ

Кирилл Валерьевич Акиндинов

студент

bokser6831@mail.ru

Наталья Викторовна Картечина

кандидат сельскохозяйственных наук, доцент

kartechnatali@mail.ru

Олег Викторович Тарасов

старший преподаватель

olegytarasovyandex.ru@mail.ru

Мичуринский государственный аграрный университет

г. Мичуринск, Россия

Аннотация. В статье рассматриваются понятия информационной безопасности, различные принципы её защиты, проблемы и их решения.

Ключевые слова: информационная безопасность, личная информация, мошенники, ИБ-специалисты.

Информационная безопасность (ИБ)– это состояние системы, при котором её части, например оборудование, каналы данных, базы данных устойчивы ко всем видам угроз.

Следует особо отметить, что корпоративные системы и личная информация пользователей в наше время требует применения мер усиленной защиты.

Личная информация пользователей, например, реквизиты банковской карты, контактные данные, информация о записи к врачу могут находиться под угрозой [3]. Сайты, на которых расположена эта информация, также как и сами аккаунты пользователей могут быть подвержены атакам вредоносного программного обеспечения и хакеров, что в последствии используют кибермошенники для осуществления различных схем по обману населения.

Изучим официальные данные о мошенничестве за последние годы:

- по информации сбербанка, с 2020 по 2023 год количество мошеннических записей увеличилось в 6 раз. В 2022 году было 500 млн таких записей, а в 2023 году – 1,5 млрд;

- в 2023 кибермошенники похитили у россиян 15,8 млрд рублей. Злоумышленники смогли провести 1,18 млн таких операций, что на 33% больше, чем в предыдущем году. При этом банки смогли отразить почти 35 млн попыток украсть деньги у граждан за 2023 год;

- по данным Роскомнадзора, за 2022 год в России произошло 140 крупных утечек, а в 2023 году -168, по итогам которых в открытый доступ попало более 500 млн записей о гражданах РФ [1,4].

Информационную безопасность также можно рассматривать, как область знаний и профессиональное направление, специалисты которого изучают уязвимости в системах и находят решения повышения их защищенности.

Сейчас ИБ-специалисты очень востребованы. Следует отметить, что спектр их компетенций достаточно сильно вырос: необходимо не только знать

вид угроз и способы защиты от них, но и владеть навыками разработчиков и аналитиков данных.



Рисунок 1 – Принципы защиты информации.

Принципы защиты информации представлены на рисунке 1. Рассмотрим подробно каждый из них.

Конфиденциальность. Вся информация должна находиться под защитой от несанкционированного получения ее. Например, на предприятиях или офисах, работа на которых происходит только с производственных компьютеров, мобильных планшетов введена документация о неразглашении информации, коммерческой тайны, конфиденциальных данных и т.д.

Целостность. Данный принцип означает, что данные являются достоверными, полными и не были случайно изменены или модифицированы неавторизованным пользователем.

Доступность. Сотрудники, у которых есть доступ к определенной информации, могут обращаться к ней по мере решения рабочих задач. При этом должны быть исключены ситуации, когда доступ к ней резко пропадает.

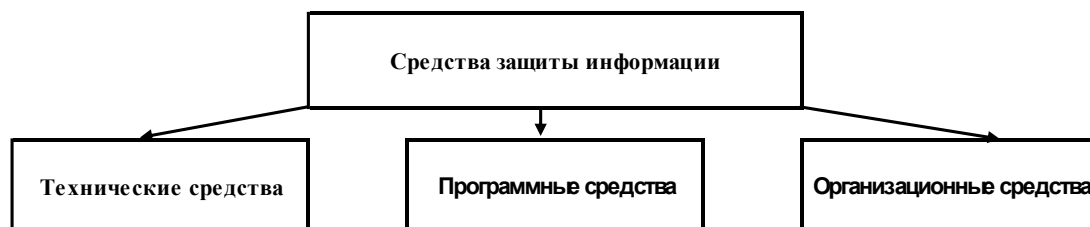


Рисунок 2 – Средства защиты информации.

Средства защиты информации представлены на схеме (рисунок 2). Рассмотрим их подробнее.

Технические средства. Это методы защиты информации, которые ограничивают доступ к ней различными способами. Например, пароль на сайте или код доступа на мобильном устройстве, которые защитят личные данные в случае потери или кражи телефона.

Программные средства. Это специализированные программы, которые могут обнаружить и предотвратить угрозу безопасности данных пользователя. К ним относятся антивирусные программы или программы, блокирующие вторжение других людей. Например: Kaspersky Free, AVG Antivirus Free, Microsoft Defender.

Организационные средства. Это методы, которые использует руководство компании, например, корпоративная политика безопасности и её соблюдение [2, 3].

Современные проблемы ИБ:

1) Развитие хакерских групп и злоумышленников в современном обществе создают множество проблем как простому населению, так и крупным компаниям. Например, с заражённого рабочего компьютера злоумышленники могут удаленно получать важную информацию и использовать её в своих интересах.

2) Неосведомлённость населения о защите и предоставлении своей личной информации (почта, номер карты и код с обратной стороны) третьим лицам. Например, самый распространённый вид мошенничества, при котором потерпевшему звонит как бы представитель банка и сообщает, что на него «мошенники оформляют кредит», для прерывания операции нужно сказать номер карты и код с обратной стороны.

3) Нехватка высококвалифицированных ИБ-специалистов является серьёзной проблемой при защите информации и систем от кибератак и других угроз.

Таким образом, главными решениями проблем в области информационной безопасности может стать сотрудничество между компаниями и

образовательными учреждениями для создания программ обучения и развития ИБ-специалистов. А также оповещение населенияс помощью средств массовой информации, в офисах банков, в информационных мероприятиях, проводимых полицией, о видах мошенничества, в том числе связанных с информацией.

Список литературы:

1. В 2023 году в открытый доступ попало более 300 млн записей персональных данных / Frank - Media – URL: <https://frankmedia.ru/150909>

2. Экономическая безопасность в системе управления персоналом / Н. И. Руднева, С. А. Хабаров, О. И. Захарова, М. В. Подосинников // Траектории социально-экономического развития региона в условиях внешнеполитического санкционного давлени: Материалы Всероссийской (национальной) научно-практической конференции, Мичуринск-наукоград РФ, 25 апреля 2023 года / Под редакцией Н.В. Карамновой. Мичуринск: Мичуринский государственный аграрный университет. 2023. С. 233-237. EDN WBHKZI.

3. Этические проблемы цифровых технологий / К. А. Ярославцева, Н. В. Пчелинцева, И. В. Чепраков, Н. В. Картечина // Инженерное обеспечение инновационных технологий в АПК: Материалы Международной научно-практической конференции, Мичуринск-наукоград, 26–28 октября 2022 года / Под общей редакцией И.П. Криволапова. Мичуринск-наукоград: Мичуринский государственный аграрный университет. 2022. С. 255-258. EDNEKKGCS.

4. Хохлов А. А., Лыкова А. Б., Никонорова Л. И. Дипфейк и общественная безопасность // Наука и образование. 2024. Т.7. №2.

UDC 004.056

INFORMATION SECURITY: MODERN PROBLEMS AND SOLUTIONS

Kirill V. Akindinov

student

bokser6831@mail.ru

Natalia V. Kartechina

candidate of agricultural sciences, associate professor

kartechnatali@mail.ru

Oleg V. Tarasov

senior lecturer

olegytarasovyandex.ru@mail.ru

Michurinsk State Agrarian University

Michurinsk, Russia

Abstract. The article discusses the concepts of information security, various principles of its protection, problems and their solutions.

Key words: information security, personal information, fraudsters, information security specialists.

Статья поступила в редакцию 11.11.2024; одобрена после рецензирования 20.12.2024; принята к публикации 25.12.2024.

The article was submitted 11.11.2024; approved after reviewing 20.12.2024; accepted for publication 25.12.2024.