УДК 681.518

Е. Ю. Царегородцева*

ЗАЩИТА ИНФОРМАЦИИ В СОВРЕМЕННОМ ОБЩЕСТВЕ

На сегодняшний день в сфере хранения и обработки информации защита информации является ключевым направлением, которому отводится важная роль.

Цель статьи заключается в рассмотрении значения защиты информации в жизни современного общества, в выявлении проблем, связанных с защитой информации, и в определении путей их решения. С учетом поставленной цели необходимо решить следующие задачи: 1) рассмотреть понятие защиты информации и ее роль для общества; 2) выявить трудности, которые возникают при хранении информации; 3) предложить рекомендации для защиты информации в современных условиях.

КЛЮЧЕВЫЕ СЛОВА: *информационные системы, защита информации, современное общество, технологии.*

E. Yu. Tsaregorodtseva

INFORMATION PROTECTION IN MODERN SOCIETY

In modern conditions, information protection in modern society is a key area, which is given great importance in the storage and processing of information.

The purpose of the article is to consider information protection in modern society with the identified problems and their subsequent solution. Based on the stated goal, the following tasks should be included: 1) to consider the concept of information protection and its role for society; 2) to identify the difficulties that society faces when storing information; 3) to offer recommendations for information protection in modern society.

KEYWORDS: *information systems, information protection, modern society, technology.*

Под защитой информации понимается деятельность по предотвращению утечки защищаемой информации, а также преднамеренного и непреднамеренного воздействия на защищаемую информацию [1, с. 739].

Защита информации предполагает существование комплекса различных мероприятий, которые направлены на обеспечение безопасности

* ***Царегородцева Елена Юрьевна****, кандидат экономических наук, доцент Иркутского государственного университета путей сообщения.*

определенной информации в государственных структурах, на предприятиях, а также в жизнедеятельности общества в целом.

Защита информации задействована при осуществлении управленческих решений, в управлении бизнес-процессами и т. д. Чтобы обезопасить данные, применяется система защиты информации, которая включает определенные органы и исполнителей, используемую ими технику защиты информации, средства программного и технического обеспечения, организованная и функционирующая по правилам, установленным правовыми, распорядительными и нормативными документами в области обеспечения безопасности данных [2]. При этом информация чаще подлежит утечке, если она конфиденциальная. В случае нарушения конфиденциальности информации наступает уголовная ответственность. Поскольку в основном утечка информации происходит в результате действий сотрудников организаций, необходимо осуществлять различные организационные мероприятия для сохранения информации.

В соответствии с федеральным законом «Об информации, информационных технологиях и о защите информации» в определении защиты информации используются такие категории, как информационные технологии и технические средства, которые помогают с помощью кодирования и шифрования обезопасить информационный поток [3].

Следует согласиться с мнением специалистов, которые утверждают: «Технические средства защиты информации включают активные и пассивные методы. Широко применяются технические меры, основанные на использовании специальных материалов и средств, технико-информационных и конструкторских решений. Производится и совершенствуется широкий ассортимент средств, позволяющих решать актуальные задачи защиты информации в помещениях и значительно усложнять перехват в условиях, специально не предназначенных для ведения конфиденциальных переговоров» [4, с. 20].

Ф. А. Капустин под информационной безопасностью предлагает понимать «состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере. Чтобы обеспечить информационную безопасность, государство ведет постоянную борьбу против внутренних и внешних угроз информационного пространства современного общества» [1].

За три года после начала СВО в России весьма обострилась проблема защиты информации, которая связана с применением иностранного программного обеспечения. По причине применения западными странами санкций к нашей стране у нас сложилась ситуация, когда все программное обеспечение, пришедшее из стран Запада со всей сопро-

вождающей документаций, схемами, чертежами, подготовленными исключительно на лицензионном ПО, в нашем государстве перестало функционировать на полную мощность. До этого времени никто не думал, что использование программного обеспечения может стать объектом санкций против России.

Что касается банковских сервисов, то Россия смогла обеспечить безопасность информации по расчетам со своими клиентами, при осуществлении транзакций. Но более серьезной остается проблема защиты персональных данных граждан и личной информации. Не секрет, что имеет место утечка персональных данных, которыми пользуются мошенники с целью выудить пароли для входа в личные кабинеты граждан в различных системах.

Рассмотрим виды информационных угроз в современном обществе (рис. 1).

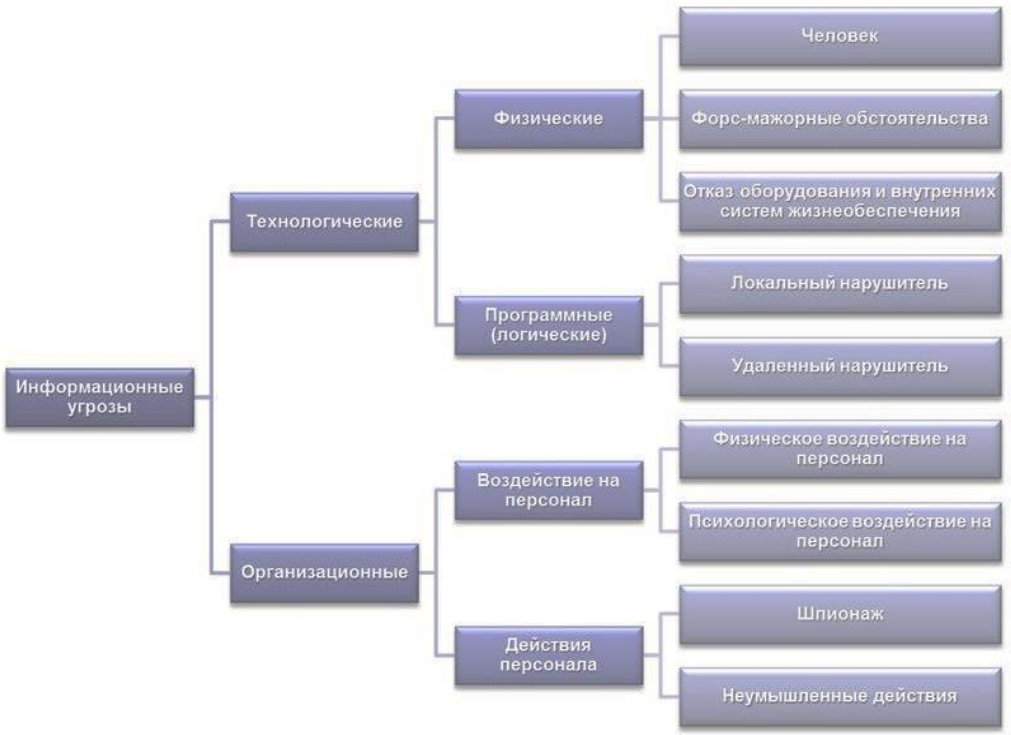

Рис. 1. Виды информационных угроз в современном обществе [5, с. 145]

Из рис. 1 становится понятно, что информационные угрозы разделяются на технологические и организационные. Технологические включают форс-мажорные обстоятельства, такие как отказ оборудования, локальные нарушения. Организационные угрозы связаны с воздействием

на персонал и могут включать физическое или психологическое воздействие на него, шпионаж и др.

В данном случае прослеживается проблема развития кибернетических криминальных сервисов, которые позволяют сделать заказ на взлом аккаунта в социальных сетях или проведение DDoS-атаки на сайт конкурента. Причем сделать это можно так же легко, как осуществить выпуск новой банковской карты или оформить подписку на онлайн-кинотеатр. Следует подчеркнуть, что в 2022 г. ситуация усугубилась, так как цены на такие, мягко выражаясь, услуги упали до минимальных значений.

В соответствии с информацией от Positive Technologies, количество угрожающей информации в Telegram в 2023 г. увеличилось в 2,5 раза, если сравнивать с довоенным периодом. В мессенджерах возникли десятки больших сообществ, которые предлагают организовывать мощнейшие DDoS-атаки за 50 долл. в сутки.

Применение методов защиты информации (рис. 2) немного ослабляет действие угроз. Данные методы делятся на две большие группы: организационно-правовые и инженерно-технические.

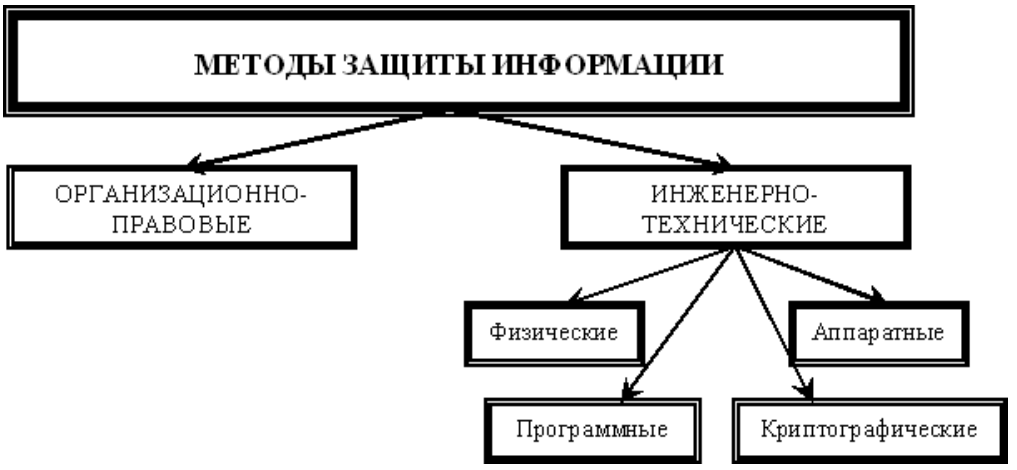

Рис. 2. Методы защиты информации [5, с. 144]

Организационно-правовые методы защиты информации предполагают выработку таких локальных актов, как положение об обработке персональных данных, положение о защите персональных данных, регламентирующих политику обработки персональных данных на предприятии, в организации.

Инженерно-техническая защита информации подразумевает использование комплекса технических средств и мер с целью предотвра-

щения утечки, распространения информации, несанкционированного доступа в сетевое пространство предприятия, организации.

Среди инженерно-технических методов защиты информации следует выделить криптографический метод, заключающийся в выработке и применении определенных алгоритмов для обеспечения конфиденциальности, целостности, аутентификации и доступности данных.

С учетом обозначенных проблем следует понимать, что основная задача государства заключается в обеспечении защиты информации от внешних и внутренних воздействий. Для этого применяются достаточно простые, но эффективные меры: выстраивание системы разграничения критичных полномочий в бизнес-системах, ограничение доступа к информационным ресурсам, превышающим минимально достаточный уровень.

Положительные моменты в области информационной безопасности могут наступить только благодаря использованию комплексного подхода, направленного на повышение эффективности обеспечения безопасности информации. При этом в законодательстве должен быть закреплен тотальный контроль со стороны государства за уровнем информационной безопасности. Адаптация традиционных мер – применение сетевых решений, повышение качества сбора оперативной информации, моделирование угроз, повышение ответственности – также расширяет границы «безопасного периметра» и создает условия для эффективного и безопасного использования информации в режиме реального времени.

Более наглядно перспективы защиты информации на период до 2030 г. представлены на рис. 3.

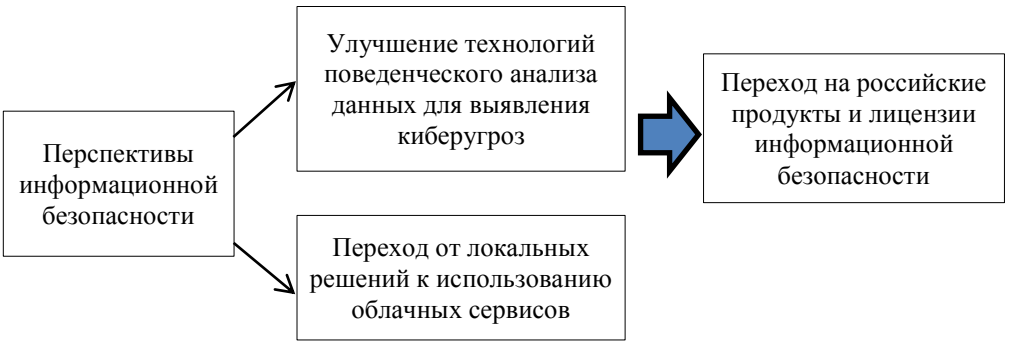

Рис. 3. Перспективы развития информационной безопасности на период до 2030 г. [2]

Развитие новых направлений в сфере обеспечения информационной безопасности следует принять во внимание при проведении обуче-

ния и повышении квалификации в области защиты информации, при разработке новых образовательных программ.

Минцифры РФ планирует до 2030 г. осуществить инвестиции в развитие отечественных технологий по обеспечению информационной безопасности в размере 25 млрд р. При этом российские эксперты рассчитывают, что в результате все иностранные средства защиты информации будут заменены российскими аналогами, а количество случаев, которые связаны с нарушением информационной безопасности, сойдет на нет [2].

Таким образом, защита информации в современных условиях имеет немаловажное значение. Число кибератак с каждым днем растет, и обеспечение информационной безопасности становится одним из приоритетных направлений. Сегодня возросла потребность в разработке и применении новых методов защиты информации. Современным организациям следует подходить к защите информации комплексно с учетом современных реалий.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. *Капустин Ф. А.* Информационная безопасность и защита информации в современном обществе / Ф. А. Капустин // Актуальные проблемы авиации и космонавтики. 2016. Т. 2. С. 738–740.
2. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : указ Президента РФ от 9 мая 2017 г. № 203 // СПС «КонсультантПлюс».
3. Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ // СПС «КонсультантПлюс».
4. *Вавилова Е. Ю.* Векторы защиты информации в современном обществе / Е. Ю. Вавилова, А. В. Кузин // Исследования молодых ученых : материалы IX Междунар. науч. конф. (г. Казань, апр. 2020 г.). Казань : Молодой ученый, 2020. С. 19–21. URL: https://moluch.ru/conf/stud/archive/368/15712.
5. *Царегородцева Е. Ю.* Значение информационных систем для современного общества / Е. Ю. Царегородцева. EDN BFPWKJ // Культура. Наука. Образование. 2024. № 2 (71). С. 143–148.