УДК 681.518

Е. Ю. Царегородцева*

СОВРЕМЕННЫЕ МЕТОДЫ ЗАЩИТЫ ОТ ЗЛОУМЫШЛЕННИКОВ

На сегодняшний день обеспечение информационной безопасности современного общества является ключевым сегментом в сфере защиты информационных ресурсов от несанкционированного доступа, в связи с чем целью статьи является изучение новых методов защиты информации от злоумышленников. Для достижения поставленной цели в статье решаются следующие задачи: 1) изучение понятия информационной безопасности с акцентом на ее роль в образовательном процессе; 2) анализ существующих киберугроз и методов защиты от них; 3) формулирование новых способов защиты от несанкционированного доступа к информации.

КЛЮЧЕВЫЕ СЛОВА: *методы защиты, современное общество, киберугрозы, инновационные технологии.*

E. Yu. Tsaregorodtseva

NEW METHODS OF PROTECTION FROM INVADERS MODERN SOCIETY

Today, information security for modern society is a key segment that plays an important role in protecting data from unauthorized access in the storage and processing of information resources. The purpose of the article is to study new methods of protection against intruders in modern society. In connection with the stated goal, the tasks will be: 1) study the concept of information security and its role in the educational process; 2) consider cyber threats and methods of protection; 3) suggest new technologies for protection against intruders.

KEYWORDS: *protection methods, modern society, cyber threats, innovative technologies.*

Обеспечение защиты своих данных в современных условиях становится все более актуальным. С каждым годом количество кибератак растет, увеличивается и их сложность. Необходимо понимать, что наряду с защитой личной информации от цифровых угроз важно создать безопасную среду для бизнеса, предотвратить возможные финансовые

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

потери и т. д. В этом контексте необходимо рассмотреть текущие вызовы, с которыми сталкиваются организации и частные лица.

Современные технологии и интернет-сервисы предоставляют множество возможностей для бизнеса и частных пользователей, но они также создают новые уязвимости. Следует осознавать, что киберугрозы могут затронуть интересы не только крупных корпораций, но и малого бизнеса, а также обычных пользователей. Например, утечка личных данных может привести к финансовым потерям и репутационным рискам. В этом контексте понимание текущих тенденций и вызовов в области кибербезопасности становится критически важным направлением.

Следует согласиться с основным положением о защите национальных интересов Доктрины информационной безопасности Российской Федерации в информационном обществе, которая определяет интересы личности, общества и государственных структур в целом [1]. В соответствии с Доктриной информационной безопасности Российской Федерации защита личности, общества и государственных структур от внешних и внутренних угроз является первостепенной задачей в реализации конституционных прав и свободы личности для сохранения достойного качества и уровня жизни населения вместе со всем социально-экономическим развитием отечественного сектора.

Ключевые виды угроз информационной безопасности можно рассмотреть на рис. 1.

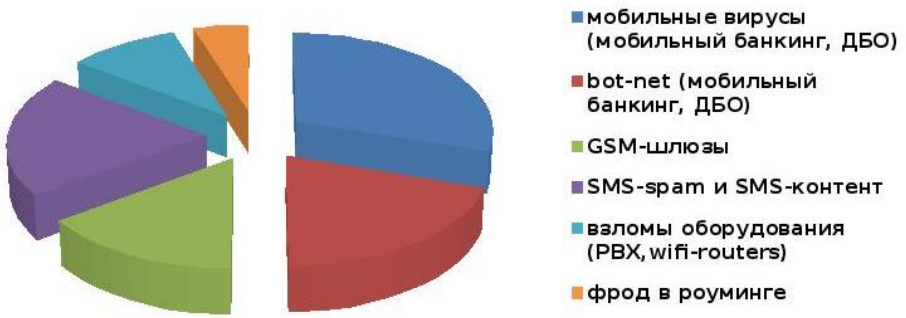

Рис. 1. Виды киберугроз для современного общества [2]

Атаки на информацию со стороны злоумышленников становятся все более распространенными. Мошенники проникают в системы через уязвимости в программном обеспечении поставщиков. Примером такой атаки является инцидент с SolarWinds, когда хакеры внедрили вредоносный код в обновления программного обеспечения, что позволило им получить доступ к системам множества компаний и государственных учреждений.

В широком смысле информационная безопасность представляет собой состояние общества, при котором обеспечивается комплексная защита как личности, так и государства от различных угроз, связанных с организованными информационными потоками. Узкое понимание информационной безопасности связано непосредственно с защитой самой информации и ее передачей. Для образовательной среды более актуально узкое определение, которое включает два ключевых аспекта исследования: безопасность формирующейся личности и безопасность уже сформировавшейся личности.

Фишинг является распространенным методом кибератак. Злоумышленники применяют разные методы, чтобы обманом заставить пользователей предоставлять конфиденциальные данные. Например, они могут отправить электронное письмо, которое выглядит как сообщение от банка, с просьбой ввести логин и пароль на поддельном сайте.

Также следует к угрозам отнести рансомваре-атаки, которые являются все более сложными и целенаправленными. Злоумышленники могут использовать различные методы для проникновения в системы, включая фишинг, уязвимости в программном обеспечении и атаки на цепочку поставок. Важно отметить, что даже если организация платит выкуп, нет гарантии, что данные будут восстановлены. Это делает рансомваре одной из самых серьезных угроз для бизнеса и частных лиц [3].

Система защиты информации представляет собой совокупность организационных и технических мероприятий, направленных на гарантирование безопасности определенной информации в государственных структурах, на предприятиях, а также для общества в целом.

Для защиты от злоумышленников следует применить следующие меры защиты конфиденциальных данных, которые представлены на рис. 2.

Рис. 2. Методы защиты от киберугроз [4, с. 419]

Из рис. 2 становится понятно, что обучение сотрудников основам кибербезопасности является ключевым направлением минимизации кибератак. При этом регулярные тренинги в распознавании фишинговых писем помогут существенно уменьшить риски от действий злоумышленников.

Помимо представленных мероприятий по защите данных, в практике используют блокчейн-технологии, которые помогают снижать риски утечки информации из центральных баз данных, например из банковской системы, где хранятся финансовые ресурсы населения.

Биометрические технологии, такие как отпечатки пальцев, распознавание лиц, являются спасением от киберугроз, поскольку на сегодняшний день биометрические данные невозможно подделать.

Доведение до населения информации о способах защиты от киберугроз является первостепенной задачей в современном обществе. Каждый гражданин должен быть осведомлен о возможных мошеннических действиях и методах защиты от них, чтобы быстро отреагировать на потенциальные угрозы, поскольку с каждым разом появляются новые способы завладеть конфиденциальной информацией со стороны злоумышленников.

Обучение в области информационной безопасности предполагает не только выявление, но и минимизацию потенциальной угрозы информационных воздействий [5, с. 143].

Подведем итоги. Современные технологии и интернет-сервисы предоставляют множество возможностей для бизнеса и частных пользователей, но они также создают новые уязвимости. Важно осознавать, что киберугрозы могут затронуть не только крупные корпорации, но и малый бизнес, а также обычных пользователей.

Кибербезопастность является комплексной проблемой, которая требует от государства разрешения данного вопроса в виде ужесточения законодательства, усиления контроля за финансовыми операциями в банковской системе, внедрения представленных в данной статье технологий, которые будут помогать снизить угрозы для современного общества [1]. При этом следует понимать, что защита от злоумышленников – это непрерывный процесс, требующий постоянной адаптации и совершенствования.

Эффективная защита должна быть многоуровневой и включать в себя технологические, организационные и человеческие факторы.

Ключевым сегментом успеха является повышение осведомленности всех членов общества о существующих угрозах и способах защиты от них [6, с. 10; 7]. Благодаря собственным усилиям можно создать безопасное цифровое пространство.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 5 дек. 2016 г. № 646. URL: https://www.garant.ru/products/ipo/prime/doc/71456224.
2. *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.
3. *Абдуллаев Э. А.* Кибербезопасность: вызовы и стратегии защиты в цифровую эпоху / Э. А. Абдуллаев // Молодой ученый. 2023. № 33 (480). С. 8–9. URL: https://moluch.ru/archive/480/105493.
4. *Писарева О. М.* Определение состава участников программ развития в цифровой среде системы стратегического планирования / О. М. Писарева // Стратегическое планирование и развитие предприятий : материалы XXIII Всерос. симпозиума. М., 2022. С. 419–422.
5. *Царегородцева Е. Ю.* Значение информационных систем для современного общества / Е. Ю. Царегородцева // Культура. Наука. Образование. 2024. № 2 (71). С. 143–148.
6. *Агеева Е. Л.* Основные аспекты информационной безопасности в образовательной среде / Е. Л. Агеева, О. Ю. Вдовина, А. Ю. Костюнин // Проблемы современного педагогического образования : сб. науч. тр. Ялта : РИО ГПА, 2021. Вып. 73, ч. 1. С. 10–12. URL: http://elibrary.udsu.ru/xmlui/bitstream/handle/123456789/20735/58.pdf?sequence=1.
7. *Утегенов Н. Б.* Рост угроз кибербезопасности / Н. Б. Утегенов // Universum: технические науки : электрон. науч. журн. 2023. № 7 (112). URL: https://7universum.com/ru/tech/archive/item/15797.