ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ

INFORMATION SECURITY IN EDUCATIONAL

Р. Р. Волоцкова, О. А. Буланкина

Институт нефтепереработки и нефтехимии
ФГБОУ ВО УГНТУ в Салавате
Салават, Россия
Institute of Oil Refining and Petrochemistry
FGBOU IN USNTU in Salavat
Salavat, Russia

e-mail: fmfizika13@yandex.ru

В статье рассмотрено развитие информационных технологий и исходящие из этого развития последствия такие, как появление информационных угроз (потеря доступа к информационным ресурсам, уничтожение и несанкционированное распространение личных данных) и способы борьбы с ними путём развития информационной безопасности в образовательной среде.

Ключевые слова: Информационные технологии, интернет, сеть, информация, информационная безопасность, кибербезопасность.

The article deals with the development of information technologies and the consequences arising from this, such as the emergence of information threats (loss of access to information resources, destruction and unauthorized dissemination of personal data) and ways to combat them through the development of information security.

Keywords: Information technology, Internet, network, information, information security, cybersecurity.

Современное общество невозможно представить без глобальных процессов социального и экономического развития. Изменения, которые терпят все сферы человеческой жизни, тесно связаны с широким внедрением новых информационных технологий, использование которых помогает достичь высокого уровня организации процессов и систем.

Информационные технологии смогли затронуть большую часть сфер общественной жизни. Самые яркие примеры – экономика, образование и культура, образовательные заведения. В этих сферах информационные технологии открывают новые возможности в расширении зон

доступности услуг, их более высоком качестве и снижении стоимости. Такой подход даёт возможность пользователям сети использовать услуги удалённо, что значительно облегчает жизнь и делает её более комфортной, позволяя управлять многочисленными потоками информации в разы эффективнее [2, с. 126].

Однако развитие информационных технологий несёт за собой и новые трудности. По статистике первый телефон у ребенка появляется в два-три года с развивающей или отвлекающей целью. С возраста 4–6 лет телефон является с целью контроля и выявления местонахождения ребенка. Взрослые сами активно приручают ребенка к информационным технологиям. Глобальное внедрение информационных технологий подразумевает наличие и использование информационных ресурсов онлайн, а значит делает информацию, хранящуюся в интернете, уязвимой, особенно это касается незащищенные слои населения. К 11 % детей в возрасте от 11 до 14 лет за прошедший год попытались втираться в доверие незнакомые люди. Данные пользователей интернета могут быть взломаны и использованы против них. Появляются новые понятия, такие как «хакер» и «слив данных». Поэтому в настоящее время безопасность в сети – это одна из наиболее актуальных проблем общества.

Для обеспечения безопасности в интернете появилась необходимость и со стороны власти принимать соответствующие меры, поскольку защита данных в сети важна не только для обычных пользователей интернета, но и для всего государства в целом. Так органами законодательной и исполнительной власти России были приняты законы и подзаконные акты по вопросам защиты информационных ресурсов государства и их сохранности в тайне.

Из всего вышесказанного можно сделать вывод, что информационная безопасность куда сложнее, чем может показаться на первый взгляд. Поэтому над обеспечением кибербезопасности работают специально подготовленные и обученные для этого специалисты с хорошим знанием различных ПО и методов защиты от взлома [2, с. 127]. Например, как самая распространённая и основная мера защиты информации используется контроль доступа, призванный исключить несанкционированный доступ к информации [1, с. 67].

Инструменты и методы информационной безопасности направлены на противодействие информационному оружию, посредством которого не только осуществляется неправомерный доступ, но и модифицирование, копирование и уничтожение данных. Поэтому, чтобы как можно более эффективно обезопасить данные, специалисты по кибербезопасности не только обеспечивают защиту информационным ресурсам, но

и проверяют сайты на такие потенциальные нарушения, как целостность, конфиденциальность и доступность. Цифровая криминалистика – это идентификация, сбор и анализ электронных доказательств. Почти каждое преступление сегодня имеет цифровой криминалистический компонент, и эксперты по цифровой криминалистике оказывают важную помощь в расследованиях полиции. Цифровые криминалистические данные часто используются в судебных разбирательствах.

Важной частью цифровой криминалистики является анализ предполагаемых кибератак для выявления, смягчения и устранения киберугроз. Таким образом, цифровая криминалистика становится неотъемлемой частью процесса реагирования на инциденты. Цифровая криминалистика также может помочь предоставить важную информацию, необходимую аудиторам, юридическим группам и правоохранительным органам после атаки.

В информационной безопасности выделяют две разновидности защиты: активная и пассивная.

Активная защита нацелена на предупреждение несанкционированного доступа к информации. К неё относят следующие приоритеты:

- защиты личных данных, т.е. социальных ценностей и иных конфиденциальных сведений;
- эксплуатация средств информационной безопасности;
- эксплуатация и защита объектов критической инфраструктуры;
- международные интересы.

Пассивная защита распространяется на условия общественного и экономического развития. В качестве её приоритетных направлений рассматриваются: свобода обращения информации; развития культуры; развитие онлайн-демократии; развитие экономики; развитие IT-сектора; международное сотрудничество [3, с. 51].

К ключевым программно-техническим инструментам информационной безопасности относятся идентификация и аутентификация. Их сочетание даёт возможность провести процедуру авторизации, благодаря которой можно установить личность пользователя.

После успешных идентификации и аутентификации следует этап авторизации. Во время этого этапа происходить проверка введённых данных и определяется возможность доступа к данным и действиям с данными (запуск, просмотр, создание, удаление, изменение отдельных данных).

Таким образом, информационная безопасность обеспечивает пользователям сети защиту их данных в интернете и информационных ре-

сурсов, без чего в современном мире невозможно обойтись. В связи с развитием IT, применяемых во всех отраслях промышленной, политической и экономической деятельностях и областях общественной жизни, информационная безопасность стала необходимой и неотъемлемой частью современности, и её роль в жизни общества приобретает всё большее значение для государства [3, с.66].

СПИСОК ЛИТЕРАТУРЫ:

1. *Буйневич М. В.* Интеллектуальный метод визуализации взаимодействий программ в интересах аудита информационной безопасности операционной системы // Информатизация и связь. 2020. № 4. С. 67–74.
2. *Волоцкова, Р. Р.* Применение современных информационных педагогических технологий в процессе подготовки специалистов СПО / Р. Р. Волоцкова, Д. Л. З. Гесс // Современные физика, математика, цифровые и нанотехнологии в науке и образовании : Сборник тезисов I Всероссийской молодежной школы-конференции, посвященной 100-летию со дня рождения А. Д. Сахарова, Уфа, 25–27 апреля 2022 года. – Уфа: Башкирский государственный педагогический университет им. М. Акмуллы, 2022. – С. 126–128. – EDN UQFWZL.
3. *Карев А. С.* Проблемы информационной безопасности в интернете вещей // В сборнике: Интернет вещей и 5G. 2016. С. 66-70.