Ревенков Павел Владимирович
д-р экон. наук, профессор
Бердюгин Александр Александрович
аспирант
ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»
г. Москва

КИБЕРГРАМОТНОСТЬ КАК СОСТАВНАЯ ЧАСТЬ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ОБЩЕСТВА

Аннотация*: в статье рассматриваются основные причины внедрения учебных мероприятий по повышению уровня киберграмотности населения. Приведены определения понятий «киберпространство» и «кибербезопасность». Даны основные рекомендации по недопущению вирусного заражения компьютера, а также возможные способы использования зараженного компьютера киберпреступниками.*

Дополнительно предложен альтернативный взгляд на научно-технический прогресс для его объёмного восприятия.

Ключевые слова*: киберпространство, кибербезопасность, киберграмотность, компьютерные вирусы, социальная инженерия.*

Перед тем как дать определение понятия «киберграмотность» необходимо разобраться, что включают в себя понятия «киберпространство» и «кибербезопасность».

Под киберпространством чаще всего понимают среду информационного взаимодействия и обмена данными, реализуемой в компьютерных сетях и сетях связи, где элементами киберпространства являются серверы, компьютеры, телекоммуникационное оборудование, каналы связи, информационные и телекоммуникационные сети. Термин киберпространство (Cyberspace) относится к коллективной сфере компьютерных коммуникаций и был впервые использован

в 1984 году в романе Вильяма Гибсона “Neuromancer” о прямой сетевой организации искусственного интеллекта.

Под кибербезопасностью понимается комплекс мероприятий, направленных на сохранение основных свойств информации: конфиденциальности, целостности и доступности информации в киберпространстве [1, с. 3].

Конфиденциальность – это гарантия, что информация может быть прочитана и проинтерпретирована только теми людьми и процессами, которые имеют авторизацию, чтобы это делать. Обеспечение конфиденциальности включает процедуры и меры, предотвращающие раскрытие информации неавторизованными пользователями. Информация, которая может считаться конфиденциальной, также называется чувствительной. Примером может являться почтовое сообщение, которое защищено от прочтения кем бы то ни было, кроме адресата.

Целостность – это гарантирование того, что информация остается неизменной, корректной и аутентичной. Обеспечение целостности предполагает предотвращение и определение неавторизованного создания, модификации или удаления информации. Примером могут являться меры, гарантирующие, что почтовое сообщение не было изменено при пересылке.

Доступность – это гарантирование того, что авторизованные пользователи могут иметь доступ и работать с информационными активами, ресурсами и системами, которые им необходимы, при этом обеспечивается требуемая производительность. Обеспечение доступности включает меры для поддержания доступности информации, несмотря на возможность создания помех, включая отказ системы и преднамеренные попытки нарушения доступности. Примером может являться защита доступа и обеспечение пропускной способности почтового сервиса [2, с. 24].

Исходя из представленных определений можно сделать вывод, что киберграмотность – это начальные сведения об информационной безопасности, используя которые пользователь Интернета, владелец смартфона или держатель банковской карты может защитить своё киберпространство: конфиденциальные

сведения, само цифровое устройство или электронные деньги, доступ к которым организован с помощью банковской карты или смарт-устройства.

Недостаток знаний об основных способах осуществления мошенничества в Интернете и высокая латентность киберпреступлений приводит к тому, что такой вид преступлений становится одним из самых распространённых.

Согласно отчётам ФинЦЕРТ (Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России) основной причиной успешных кибератак является человеческий фактор. Именно от уровня осведомленности граждан об основных способах мошенничества с использованием цифровых устройств и глобальной сети Интернет зависит то, насколько действия кибермошенников будут успешными [5, с. 15].

Подавляющее большинство киберпреступлений начинается с заражения компьютера вредоносной программной или, говоря другими словами, вирусом. Основная цель – взять контроль над компьютером жертвы.

Чаще всего пользователь сам совершает опрометчивые шаги перед тем, как получить вирус на свой компьютер:

– переходит по подозрительным ссылкам в электронной почте или в web-браузере;

– открывает подозрительные вложения электронной почты;

– скачивает и устанавливает «пиратское» программное обеспечение или бесплатное программное обеспечение из сомнительных источников;

– не проверяет носители информации антивирусными программами, перед тем как вставить в USB-порт своего компьютера: флешки, внешние жесткие диски, SD/MMC карты, телефоны и другие устройства, на которых могут быть вирусные программы.

Добавим, что заражение также может быть и через локальную вычислительную сеть от другого заражённого устройства.

Теперь разберёмся, что может делать заражённый компьютер, а точнее сказать, что может делать вирусная программа, установленная на нём.

Во-первых, такая программа может осуществлять поиск в локальной сети интересующего злоумышленника объекта и предоставление к нему удалённого доступа через заражённое устройство. В дальнейшем злоумышленник будет стремиться похитить так называемую чувствительную информации. Это могут быть персональные данные о конкретных людях, конфиденциальная информация, которая используется при работе с банковскими приложениями, сведения, представляющие интеллектуальную собственность, и другая информация представляющая возможность злоумышленнику совершать мошеннические действия.

Во-вторых, заражённый компьютер может стать звеном ботнета (от англ. botnet, где bot – это заражённый компьютер, а net – это сеть. В результате ботнет – это сеть, состоящая из заражённых компьютеров), и в дальнейшем использоваться для организации DDoS-атак (от англ. Distributed Denial of Service, распределённый отказ в обслуживании) и рассылки спама [3, с. 215].

В-третьих, заражённый компьютер может использоваться в качестве точки распространения вредоносных компьютерных программ.

В-четвертых, такой компьютер, если на нем установлены банковские приложения, может выполнять различные расчётные операции в интересах злоумышленника.

И последнее – компьютерный вирус может нарушать одно или несколько свойств информации: целостность, конфиденциальность или доступность.

По мнению авторов, наиболее эффективным способом снижения уровня киберпреступности является повышения уровня киберграмотности граждан. Уроки по данной тематике должны стать неотъемлемой частью учебного процесса в школах и гимназиях

Наглядный примером успешной работы по данному направлению является проект «Онлайн-уроки финансовой грамотности для детей по безопасности в киберпространстве», начатый Банком России в 2019 году.

В 2019 году более 200 тыс. учеников старших классов из разных регионов страны стали слушателями подготовленных Банком России онлайн-уроков, по-

священных существующим киберугрозам в Интернете, безопасности платежей в сети и противодействию методам социальной инженерии.

Лекторами выступили ведущие специалисты ФинЦЕРТ. Организационную поддержку оказывали сотрудники Службы по защите прав потребителей и обеспечению доступности финансовых услуг Банка России.

По результатам данной работы ФинЦЕРТ получил престижную Премию Рунета в номинации «Детский Рунет» за данный проект [4, с. 102].

По мнению авторов, подобные инициативы должны стать примером для многих организаций и компаний, осуществляющих свою деятельность в киберпространстве. На занятиях могут использоваться учебник [3] и учебное пособие [4] авторов. Только совместные усилия и совместная ответственность за повышения уровня киберграмотности населения могут привести к должным результатам и существенно уменьшить возможности киберпреступников.

Киберграмотность как составную часть обеспечения кибербезопасности общества определяет научно-технический прогресс страны. В конце XX века китайские исследователи отправили делегации в Apple, Microsoft, Google – и расспросили изобретателей, которые «придумывают будущее», о них самих. Выявили общие шаблоны поведения и обнаружили, что все эти изобретатели читали в детстве научную фантастику. Воображение развивают именно книги. В школьную программу Китая по литературе срочно ввели эти книги, а сегодня электронные разработки фирм Huawei, Lenovo и Xiaomi – в числе мировых лидеров.

В головном мозгу человека существуют нервные клетки, которые отвечают за подражание и активизируются, когда мы следим за действиями других людей. Это зеркальные нейроны. Мы реально становимся неким средним арифметическим своего окружения [4, с. 103]. Но окружение может быть создано с помощью книг, музыки и фильмов.

Военная мощь России отчасти связана с военной литературой, занявшей прочные позиции после победы в Великой Отечественной войне. Произведениями «твёрдой» научной фантастики предлагается дополнить уроки литературы

и перечень «100 книг для школьника». Наравне с обязательным общим образованием мы получим альтернативный взгляд на научно-технический прогресс. Объёмность изображения человек воспринимает благодаря бинокулярному (от лат. bini – «два» и лат. oculus – «глаз») зрению. Аналогично взгляд с двух точек зрения (образование и фантастика) на цивилизацию даст её объёмное восприятие. Хорошая база заложена ещё советскими фантастами, а фундаментальное образование у нас достаточно сильное.

Список литературы

1. ISO/IEC 27032:2012. Information technology – Security techniques – Guidelines for cybersecurity. International Organization for Standardization, 2012. URL: http://www.iso.org/standard/44375.html (дата обращения: 04.04.2020).

2. Козьминых С.И. Обеспечение комплексной защиты объектов информатизации: учебное пособие. – М.: Юнити-Дана, 2020. – 543 с.

3. Криворучко С.В. Современные платежные системы и технологии: учебник / С.В. Криворучко, П.В. Ревенков, А.А. Бердюгин [и др.]; под ред. С.В. Криворучко. – М.: КноРус, 2020. – 248 с.

4. Ревенков П.В. Минимизация риска воздействия кибератак в условиях применения технологий дистанционного банковского обслуживания: учебное пособие / П.В. Ревенков, А.А. Бердюгин, И.В. Ожеред. – М.: Прометей, 2020. – 214 с.

5. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов. – М.: Центральный банк Российской Федерации, 2019. – 26 с. [Электронный ресурс]. – Режим доступа: https://www.cbr.ru/Content/Document/File/83253/onrib_2021.pdf (дата обращения 04.04.2020).

6. Долинго Б. Фантастика – самый мощный инструмент развития воображения // Наука и жизнь. – 2016. – №6. – 140 с. [Электронный ресурс]. – Режим доступа: https://www.nkj.ru/archive/articles/28924/ (дата обращения: 05.04.2020).