УДК 374

Некоторые аспекты формирования знаний в сфере информационной безопасности

Волков Максим Константинович volkovmk@student.bmstu.ru
Косовская Валентина Васильевна kosva@bmstu.ru

МГТУ им. Н.Э. Баумана, Россия, Москва

Аннотация. *Рассмотрена проблема низкого уровня знаний в сфере информационной безопасности у среднестатистического человека — пользователя. Поднята проблема необходимости повышения знаний в сфере информационной безопасности в обществе. Были описаны принципы информационной безопасности, методы и средства для их защиты. Даны простейшие рекомендации по безопасному использованию сети Интернет.*

Ключевые слова: *информационная безопасность, цифровизация, уровень знаний, информационная система, вредоносная деятельность*

Some aspects of knowledge formation in the field of information security

Volkov Maxim Konstantinovich volkovmk@student.bmstu.ru
Kosovskaya Valentina Vasilyevna kosva@bmstu.ru

BMSTU, Moscow, Russia

Abstract. *The article examines the problem of the low level of knowledge in the field of information security among the average human user. The problem of the need to increase knowledge in the field of information security in society is raised. The principles of information security, methods and means for their protection were described. The simplest recommendations for the safe use of the Internet are given.*

Keywords: *information security, digitalization, knowledge level, information system, malicious activity*

Введение. Тема защиты информации была актуальна на протяжении всего развития человечества, так как люди всегда стремились защищать важную для них информацию, об этом говорит огромное количество исторических примеров и фактов. Наиболее актуальной данная проблема стала в начале XXI века, в эпоху цифровизации и глобальной сетевой взаимосвязанности [1]. В связи с этим, информационная безопасность становится одним из ключевых приоритетов как для рядовых пользователей, так и для организаций. Современная практика показывает, что многие киберинциденты происходили не столько из-за технических уязвимостей, сколько из-за человеческого фактора и недостатка знаний у пользователей. Современные вызовы в сфере ин-

формационной безопасности требуют не только развития технологических решений, но и повышения уровня осведомленности каждого пользователя сети Интернет, за счет развития образовательных программ в сфере информационной безопасности [2]. В ногу с развитием технологий, развивается и законодательство в данной сфере, поэтому в соответствии с главой 2 Конституции Российской Федерации, граждане имеют право на тайну личной переписки, право на охрану персональных данных, право на свободу доступа к информации и т. д.

Целью работы является определение ключевых аспектов в области развития информационной безопасности, а также определение причин низкого уровня знаний в данной сфере.

Научная новизна работы заключается в совокупности следующих признаков, в первую очередь, речь идет о низком уровне знаний обычных пользователей, что является актуальной и малоизученной проблемой. Далее имеет место быть междисциплинарный подход, а именно сочетание в исследовании исторического анализа развития информационной безопасности с современными проблемами грамотности пользователей в этой сфере. И, наконец, историческая перспектива, которая представляет в себе углубление в историю информационной безопасности, что позволяет выявить корни современных проблем.

Материалы и методы. Проблема информационной безопасности стала более актуальна в связи с быстрым развитием информационных технологий и цифровизации общества. Многие аспекты нашей жизни стали наиболее зависимы от интернета и других цифровых благ цивилизации. Интернет содержит в себе огромный спектр услуг, например: электронная коммерция, банковские услуги, образовательные услуги, медицинские консультации и записи на прием, страховые услуги и т. д., и спектр услуг с каждым днем растет. «Дверью» для использования данных услуг являются интернет-приложения, другими словами информационные системы, которые так или иначе могут быть уязвимы. Кроме эксплуатации различных технических уязвимостей, злоумышленник может использовать иные вектора атак, например, социальную инженерию и другие способы. Поэтому информационная безопасность перестает быть исключительной заботой IT-специалистов [3].

Целью хакера может быть любое коммерческое веб-приложение, информационная система, сетевая инфраструктура коммерческой организации, электронные почтовые ящики пользователей и т. д. Как правило, вредоносная деятельность хакера направлена на получение материальной выгоды, для чего он может использовать разные техники, тактики и средства, например для получения персональных данных пользователей, получения контроля над атакуемой системой или для ее заражения вредоносным программным обеспечением. Подобная деятельность является результатом умственной деятельности хакера, при которой он использует свои знания в сфере информационных технологий. Описанный процесс называется кибератакой, как пишет Д.М. Берова, — «Кибератака, в узком смысле, — это покушение на компью-

терную безопасность информационной системы. В широком же смысле, кибератака рассматривается как поиск решений, методов, конечной целью которых является получение контроля над удаленной системой в целях ее дестабилизации» [4]. Существуют разные этапы кибератаки, поэтому на каждом из них, целью злоумышленника являются разные данные, например на этапе получения первоначального доступа злоумышленник будет пытаться украсть логин и пароль пользователя, после получения которых, ничего не помешает ему успешно аутентифицироваться в атакуемом приложении, после чего, хакер сможет получить другие данные пользователя, например данные банковской карты, также, возможен вариант при котором хакер повысит свои привилегии в системе и сможет украсть данные и других пользователей. Действия, направленные на компрометацию и нарушение состояния данных пользователя, нарушают основные принципы информационной безопасности, а именно:

– конфиденциальность (защита от несанкционированного получения информации);

– целостность информации (защита от несанкционированного изменения информации);

– доступность (защита от несанкционированного или случайного удержания информации и ресурсов системы).

При нарушении хотя бы одного из этих признаков, информация теряет статус защищенной, поэтому заинтересованные лица заинтересованы в обеспечении защиты своих интернет-ресурсов с использованием разных программных и аппаратных решений. Для сохранения конфиденциальности данных, используются такие технические решения как: современные алгоритмы шифрования данных, создание хеш-функций, использование электронной сертификации и т. д.

Для обеспечения целостности данных применяются: создание резервных копий, использование цифровых подписей, криптографические хеш-функции и т. д. Одним из основных подходов обеспечения целостности информации является ее резервирование [5].

Что касается обеспечения доступности, веб-приложение должно быть доступным в любое время для всех пользователей, которые имеют возможность подключаться к нему, как правило, с использованием локальных учетных записей. Поэтому приложение должно быть надежными, отказоустойчивыми, постоянно обслуживаться и обновляться, его техническое состояние должно постоянно отслеживаться и проверяться.

Результаты. Выше были перечислены некоторые методы защиты информации, с точки зрения обеспечения ее конфиденциальности, целостности и доступности. Перечисленные средства являются «верхушкой айсберга», так как в мире информационной безопасности существует гораздо больше приемов, направленных на защиту информации. Однако представленная информация позволяет понять, насколько хорошо защищены многие приложения, за счет совокупности мер обеспечения защиты информации в рамках предот-

вращения нарушения принципов информационной безопасности. Данная информация указывает на то, что многие сервисы, приложения и периферия организаций для большинства хакеров практически неуязвимы, так как программно-аппаратные средства, обеспечивающие их работу, постоянно обновляются, дорабатываются и защищаются. Однако полностью безопасных систем не существует, успех поиска той или иной уязвимости зависти от уровня подготовленности хакера. Если у него не хватает знаний и умений для поиска уязвимости в атакуемой системе, хакер будет стараться использовать другие методы получения доступа к ней, как правило, направленные на неосведомленность рядового пользователя в сфере кибербезопасности.

Проблемы низкого уровня знаний среднего пользователя в сфере информационной безопасности и методах ее защиты актуальна как никогда. Статистика показывает, что в практически в 50 % случаев взлома, «дверью» для злоумышленника служит рядовой пользователь. В атакованных европейских организациях за 2021 г., точкой входа для злоумышленника в 46 % случаев становился рядовой пользователь. В 2023 г. почти половина 43 % всех успешных атак на организации были проведены с использованием социальной инженерии, и 79 % из них осуществлялись через электронную почту, смс-сообщения, социальные сети и мессенджеры. Основной целью фишинговых атак является кража данных, что составляет 85 % инцидентов. Также статистика показывает, что 91 % всех кибератак начинаются с фишингового письма. Это подчеркивает значимость фишинга как основного метода, используемого хакерами для получения доступа к конфиденциальной информации и системам. Главный принцип фишинга описан в работе А.Л. Ермаковой и В.Н. Чаплигиной: «Одним из самых распространенных видов цифрового мошенничества является фишинг, сутью которого является под любым предлогом узнать конфиденциальную информацию с последующим использованием ее в корыстных целях» [6].

Фишинговые рассылки применяются как для получения данных обычных пользователей, так и для получения доступа к инфраструктуре атакуемой организации. Для этих целей существуют разные виды фишинга: фишинг через электронную почту, смишинг (SMS-фишинг), фишинг в социальных сетях, фишинговые сообщения через мессенджеры. Содержание таких писем может варьироваться в зависимости от цели атакующего, это может быть зараженный вредоносной программой файл, при открытии которого сработает «макрос», который активирует вирус. Вирус может содержать в себе любой функционал, однако наиболее распространены вирусы типа бэкдор. Эти программы, оказавшись на устройстве жертвы, позволят злоумышленнику собрать необходимую для достижения его цели информацию. Если речь идет об атаке на инфраструктуру компании, запуск вируса может означать получение первоначального доступа злоумышленником, после чего, он сможет повысить привилегии и нанести ущерб атакуемой системе. Также внутри фишингового письма может быть ссылка на вредоносный фишинговый сайт, который выглядит, например, как приложение

банка. Если не всматриваться в детали, сайт не отличить от оригинала, поэтому многие пользователи лишились своих денег из-за таких вредоносных сайтов, куда они ввели свои персональные данные. Кроме этого, возможен следующий вариант развития событий, при нажатии на URL, пользователя перекинет на вредоносный сайт, после чего на его устройство моментально установится вредоносная программа, о функционале которых сказано выше. Поэтому даже обыкновенный переход на какой-либо непроверенный сайт может стать причиной заражения и компрометации устройства, а если подобное произошло на рабочем компьютере, то и всей инфраструктуры. Кроме фишинга, существуют и другие техники и тактики злоумышленников, которые направленны на достижение целей хакера. В любом случае, пользователи должны быть осведомлены об этих угрозах и принимать соответствующие меры предосторожности для защиты своих персональных и рабочих данных.

В условиях постоянно растущего числа кибератак, осведомленность и проактивные меры защиты становятся не просто рекомендациями, а необходимостью. Каждый из нас может стать мишенью для злоумышленников, стремящихся украсть конфиденциальную информацию или получить доступ к финансовым средствам. Поэтому важно не только осознавать потенциальную угрозу, но и активно внедрять методы защиты в свою жизнь и работу. Начать можно с таких базовых шагов.

1. Внимательно проверяйте электронные письма, не спешите отвечать или выполнять инструкции из письма, сначала проверьте важные детали, такие как тема письма, ошибки в тексте и почтовый адрес отправителя.

2. Не теряйте бдительность в мессенджерах и социальных сетях, будьте осторожны с сообщениями и ссылками, которые вы получаете через эти каналы.

3. Перед вводом номера карты остановитесь, подумайте дважды, прежде чем вводить конфиденциальные данные на веб-сайтах, обращайте внимание на URL.

4. Используйте разные пароли для каждого аккаунта, например в разных виртуальных почтовых ящиках, используйте уникальный пароль.

5. Включите двухфакторную аутентификацию, это добавит дополнительный уровень защиты для ваших аккаунтов.

6. Для защиты от вредоносных программ используйте надежную защиту, установите антивирусные и антифишинговые программы.

7. Регулярно производите резервное копирование данных, это поможет восстановить информацию в случае ее утраты.

Обсуждение полученных результатов. В результате анализа проблемы низкого уровня знаний в сфере информационной безопасности у обычного пользователя, были определены следующие основные причины.

1. **Отсутствие осведомленности**: многие пользователи не осознают, что они могут стать жертвами киберпреступников. Они не понимают, какие угро-

зы могут возникнуть при использовании интернета, социальных сетей и электронной почты.

2. **Сложность темы**: кибербезопасность — это сложная область, которая постоянно меняется. Технологии развиваются, и новые угрозы появляются каждый день. Пользователи могут чувствовать себя потерянными в этом море терминов, концепций и технологий.

3. **Отсутствие соответствующих образовательных курсов, программ и дисциплин**, хотя каждый обучающийся должен пройти базовый курс по информационной безопасности в университете, чтобы их личные и рабочие данные были в безопасности [7, 8].

Заключение. В результате анализа данной проблемы, были определены основные причины низкого уровня знаний в сфере информационной безопасности у обычного пользователя. Также была поднята проблема необходимости повышения знаний в сфере информационной безопасности в обществе. Кроме этого, были описаны принципы информационной безопасности, методы и средства для их защиты. Также были даны простейшие рекомендации по безопасному использованию сети Интернет.

Список источников

[1] Парамонов А.В., Харин В.В. Некоторые аспекты обеспечения национальной безопасности в информационной сфере. *Актуальные проблемы государства и права*, 2021, т. 5, № 17, с. 161–170. https://doi.org/10.20310/2587-9340-2021-5-17-161-170

[2] Чурилина В.В. Модель управления знаниями в сфере информационной безопасности в организации. *Опыт и перспективы совершенствования систем связи и автоматизации. Всерос. науч.-практ. конф.: сб. тр.* Санкт-Петербург, 2024, с. 336–339.

[3] Цибизова Т.Ю., Слепцова К.А. Автоматизированная система учета данных внутрикорпоративной сети управления информацией. *Современные проблемы науки и образования*, 2015, № 1-1. URL: https://science-education.ru/ru/article/view?id=19593 (дата обращения 12.11.2025).

[4] Берова Д.М. Кибератаки как угроза информационной безопасности. *Пробелы в российском законодательстве*, 2018, № 2, с. 186–188.

[5] Пушкарев А.В., Новиков С.Н. Исследование методов обеспечения целостности информации в информационных системах с оптическими каналами связи. *Интерэкспо ГеоСибирь*, 2020, т. 6, № 2, с. 66–71. https://doi.org/10.33764/2618-981X-2020-6-2-66-71

[6] Ермакова А.Л., Чаплыгина В.Н. Фишинг как распространенное киберпреступление современности. *Закон и право*, 2022, № 2, с. 149–151. https://doi.org/10.24412/2073-3313-2022-2-149-151

[7] Козырев С.И. Некоторые аспекты преподавания дисциплины «Информационная безопасность» в разрезе формирования профессиональных качеств специалистов и вызовов современности. *Вопросы педагогики*, 2022, № 3-1, с. 123–128.

[8] Худяков В.В. Совершенствование знаний в сфере информационной безопасности в рамках интеграции с учебными дисциплинами. *Проблемы теории и практики инновационного развития и интеграции современной науки и образования. V Междунар. науч.-практ. конф.: матер.* Москва, ООО «Принтика» 2024, с. 172–176.