8. *Лагута Л.М.* Трансформация социальных ценностей студенческой молодежи // Актуальные проблемы социально–гуманитарных наук. Материалы Всеукраинской научной конференции. – Днепропетровск: «Инновация», 2011. – С. 39-46.
9. *Палфри Дж., Гассер У.* Дети цифровой эры. – М.: Эксмо, 2011. – 368 с.
10. *Пивоваров Д.В.* Философия религии: учеб. пособие. – М.: Акад. Проект; Екатеринбург: Деловая книга, 2006. – 640 с.
11. *Тощенко Ж.Т.* Парадоксальный человек. – М.: «Гардарики», 2001. – 398 с.
12. Ценностные ориентации российской молодежи и реализация государственной молодежной политики: результаты исследования: монография / Государственный университет управления; [под общ. ред. С.В. Чуева]. – М.: Издательский дом ГУУ, 2017. – 131 с.
13. *Чернышева А.В.* Изменение общечеловеческих ценностей как результат социокультурных трансформаций эпохи глобализации // Человек. Общество. Инклюзия. – 2016. – № 3(27). Часть 1. – С. 78-90.

TRANSFORMATION OF SPIRITUAL VALUES OF YOUTH DURING THE PERIOD OF TRANSITION TO THE INFORMATION SOCIETY

CHERNYSHEVA Anna Vladimirovna
PhD in Philosophy, Associate Professor
LAKSHINA Sofia Evgenievna
student
N.E. Bauman's Moscow State Technical University
Moscow, Russia

The article is devoted to the analysis of the process of transformation of the value system of youth, during which there is a break in the declared values and life orientations that determine the behavior of young people, and they come to the conclusion that the worldview of modern youth is synthetic: it contains, on the one hand, conservative values, focusing on stability and communication between generations, on the other – «modernist» attitudes, reflecting modern social realities.
Key words: identification, globalization, multicultural environment, informatization, modernization, spiritual life, values, youth.

ФИШИНГ КАК УГРОЗА СОВРЕМЕННОМУ ИНФОРМАЦИОННОМУ ОБЩЕСТВУ

ЧЕРНЫШЕВА Анна Владимировна
кандидат философских наук, доцент
САМОЙЛОВ Савва Игоревич
студент
ФГБОУ ВО «Московский государственный технический университет им. Н.Э. Баумана»
г. Москва, Россия

Современному информационному обществу сложно представить себе жизнь без взаимодействия с интернетом. Однако мошенничество не обошло стороной и информационное поле. В данной статье мы рассмотрим один из видов финансово-ориентированного киберпреступления, который называется фишинг. Особенностью данной мошеннической схемы является принуждение получателя электронного письма к переходу по ссылке от имени легитимной организации с целью получения личных данных жертвы.
Ключевые слова: киберперсутпность, киберпреступления, фишинг, фишинговая компания, методы борьбы, информация.

Развитие научно-технического прогресса, связанное с внедрением современных информационных технологий, привело к появлению новых видов преступлений, в частности, к незаконному вмешательству в работу электронно-вычислительных машин, систем и компьютерных сетей, хищению, присвоению, вымогательству компьютерной информации, опасному противообщественному явлению, получившему название – киберперступность.

Таким образом, киберпретсупление – это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства [7]. Большинство киберпреступлений совершаются киберпреступниками или хакерами, основной мотивацией которых является получение денег. Такая деятельность может осуществляться отдельными лицами или организациями, которые основывают киберперступники. Однако целью преступников в информационной среде может быть не только жажда прибыли. Также киберпреступления могут совершаться ради достижения экономических целей, таких как, нанесение экономического ущерба в виде воровства денежных средств и конфиденциальной информации. К другим видам целей относятся политические – нанесение ущерба основным государственным и политическим институтам, идеологические – распространение идей и идеологий с целью вербовки интернет-пользователей в ряды, например, террористических группировок. И, наконец, социально-психологические, наносящие моральный и психологический вред гражданам. Все вышеизложенное позволяет нам говорить о том, что объектами воздействия киберпреступников могут быть простые граждане, организации, государственные институты, а также их личная информация, свобода и персональная кибербезопасность.

Итак, мы дали общую характеристику киберперступности и киберпреступлениям, в дальнейшем мы проанализируем один из самых распространенных типов киберпреступлений – фишинг. Фишинг – это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователя, например, логинам и паролям. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов. Письма содержат в себе прямую ссылку на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. Редирект – это перенаправление пользователя с одной страницы на другую (с одного URL на другой). Следует подчеркнуть, что редиректы могут перенаправлять посетителей как на страницы того же сайта, так и на страницы другого сайта. Вернемся к вопросу о схеме действия фишинга. После того как пользователь попадает на поддельную страницу, интернет-мошенники пытаются различными психологическими приемами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определенному сайту, что позволяет мошенникам получить доступ к личной информации и банковским счетам своей жертвы. Самое нашумевшее и масштабное использование фишинг-мошенничества произошло в 2018 году на Чемпионате мира по футболу в России. По информации Inc, фишинговые электронные письма рассылались футбольным фанатам. В этих письмах интернет-мошенники соблазняли болельщиков фальшивыми бесплатными поездками в Москву на Чемпионат мира. У людей, которые переходили по фишинговой ссылке в сообщениях, были украдены личные данные. На основании вышесказанного можно сделать вывод, что фишинговая компания – это массовая рассылка спам-сообщений или других форм коммуникации с целью заставить получателей выполнить действия, которые ставят под угрозу их личную безопасность или опасность организации, в которой они работают [7]. Кроме того, сообщения в фишинговой рассылке могут содержать зараженные вложения или ссылки на вредоносные сайты. Они также могут просить получателя в ответном письме предоставить конфиденциальную инфомрацию. Рассмотрим такое понятие как социальная инженерия. Социальная инженерия – это метод манипуляции действиями человека, заключающийся в ис-

пользовании слабостей человеческого фактора в целях незаконного получения личной информации, например, банковские данные или несанкционированного доступа к компьютеру жертвы с целью установки на него вредоносного ПО [6]. Атака с использованием вредоносного ПО – это заражение компьютерной системы или сети компьютерным вирусом или другим типом вредоносного ПО. В свою очередь компьютер, зараженный вредоносной программой, может использоваться интернет-мошенниками для достижения различных целей. К ним относятся кража конфиденциальных данных, использование компьютера для совершения других преступных действий или нанесение ущерба данным. Известным примером атаки с использованием вредоносного ПО является атака WannaCry – это тип программ-вымогателей, которые используют уязвимость компьютеров на операционной система Windows. В мае 2017 года жертвами WannaCry стали 230 000 компьютеров в 150 странах мира. Владельцы заблокированных файлов отправили сообщение с согласием заплатить выкуп за восстановление доступа к своим данным. Финансовые потери в результате деятельности WannaCry оцениваются в 4 миллиарда долларов. Обобщая все вышесказанное, приходим к следующему выводу: фишинг – одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности: в частности, многие люди не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учетные данные, пароли и логины.

Определив сущность феномена фишинг, рассмотрим не менее важную проблему – причины увеличения количества киберперступлений. Мы считаем, что самая основная причина увеличения киберпреступлений – это развитие научно-технического прогресса. Потому что использование информационных технологий расширяет свое действие на все новые сферы человеческой деятельности, например контроль за воздушным и наземным транспортом. Выход деятельности людей в информационное поле, не мог не привлечь внимание мошенников. Поэтому развитие научно-технического прогресса, связанное с внедрением современных информационных технологий, привело к увеличению и появлению новых видов киберпреступлений.

В начале 2020 г. начинает распространяться новый вирус, получивший название COVID-19. Вследствие этого деятельность многих людей перешла в информационное пространство. Большинство учреждений перешло на дистанционный формат работы или обучений, также стали популярными онлайн-покупки в интернет-магазинах и курьерские доставки. Сложившаяся ситуация не осталась без внимания интернет-мошенников. Поскольку информацию в интернете невозможно контролировать, он остается местом, где пользователь рискует нарваться на множество проблем, в нашем случае это поддельный сайт. Задачей поддельных сайтов является использование личных данных пользователей реальных сайтов в преступных целях. Такие сайты-подделки создаются как подделки популярных веб-ресурсов, которым пользователи доверяют. Практически всегда дизайн сайтов-подделок напоминает или даже бывает идентичен дизайну реального популярного сайта. Такие сайты опасны следующим – кражей личных данных пользователей (паролей, логинов или пинкодов); распространением вредоносных ПО; навязыванием платных услуг.

Подобная схема фишинга начинается с того, что на почту пользователя приходит электронное письмо со ссылкой на фальшивый сайт. Такое письмо замаскировано под сообщение банка или другой узнаваемой организации. В нем очень убедительно и порой грозно говорится, что с вашей учетной записью проблемы, что она может быть заблокирована или любая другая причина, побуждающая перейти на сайт по ссылке. Если перейти по фишинговой-ссылке и ввести свои личные данные, то, скорее всего, они будут украдены.

Руководитель следственного департамента МВД России С. Лебедев считает, что рост киберпреступлений на территории России связан в том числе с распространением коронавируса, когда многие сферы общественных отношений переместились в интернет-пространство. «И не в последнюю очередь на

это повлияли последствия распространения коронавирусной инфекции COVID-19, в частности переход многих сфер общественных отношений, включая удаленный режим работы, товарный и денежный обороты, в интернет-пространство», – заявил он в интервью газете «Коммерсантъ». Также он рассказал, что именно нарастающее использование онлайн сервисов обуславливает постоянный и значительный рост числа преступлений, совершенных с использованием IT-технологий. Ранее в МВД сообщали, что проблемой остается рост IT-преступлений. Их количество, по данным ведомства, в 2020 году возросло на 76,7%, в том числе с использованием сети интернет – на 90,2%, с использованием средств мобильной связи – на 100,5% [5].

Таким образом, мы выяснили, что причиной увеличения количества киберпреступлений является технологический прогресс и вирус COVID-19. Данные явления связаны тем, что они оба побуждают людей чаще взаимодействовать с интернетом, проводить в нем свое свободное время, работать или учиться. В свою очередь интернет-мошенники этим пользуются, поэтому увеличиваются количества киберпреступлений.

Следует отметить, что существуют различные методы для борьбы с фишингом, включая законодательные меры и специальные технологии, созданные для защиты от фишинга. Например, для защиты такого рода мошенничества производители основных интернет-браузеров договорились о применении одинаковых способов информирования пользователей о том, что они открыли подозрительный сайт, который может принадлежать мошенникам. Новые версии браузеров уже обладают такой возможностью, которая соответственно именуется «антифишинг». Самый простой способ метода борьбы с фишингом заключается в том, чтобы научить людей различать фишинг и бороться с ним. Люди могут самостоятельно снизить угрозу фишинга просто выполняя следующие действия. В ответ на письмо с просьбой «подтверждения» учетной записи можно связаться с компанией, от имени которой отправлено сообщение, для проверки его подлинности. Кроме того, рекомендуется самостоятельно вводить веб-адрес организации в адресную строку браузера вместо использования любых гиперссылок в подозрительном сообщении. Для того, чтобы не стать жертвой интернет-мошенников достаточно следовать следующим правилам компьютерной безопасности:

1. Не переходите по присылаемой ссылке от незнакомых людей и не просматривайте файлы. Классический способ заражения компьютеров с помощью вредоносных атак и других типов киберпреступлений – это вложения в электронных спам-сообщениях. Никогда не открывайте вложение от неизвестного вам отправителя.

2. Если на почту пришло подозрительное письмо от лица известной компании, лучше связаться с ними по телефону, указанному на официальном сайте компании и убедитесь, что вам звонили не мошенники.

3. Не нажимайте на ссылки в электронных спам-сообщениях и на сайтах, которым не доверяете. Один из способов, используемый киберпреступниками для заражения компьютеров пользователей, – это вредоносные ссылки в спамовых электронных письмах или других сообщениях, а также на незаконных веб-сайтах.

4. Не предоставляйте личную информацию, не убедившись в безопасности канала передачи. Никогда не передавайте личные данные по телефону или по электронной почте, если вы не уверены, что телефонные соединение или электронная почта защищены. Убедитесь, что вы действительно говорите именно с тем человеком, который вам нужен.

5. Не посещайте вредоносные сайты. Внимательно проверяйте адреса веб-сайтов, которые вы посещаете. Обращайте внимание на URL-адреса сайтов, на которые вы хотите зайти. Они должны выглядеть легитимно. Ни в коем случае не переходите по ссылкам, содержащим незнакомые или на вид спамовые URL-адреса. Также если ваш продукт для обеспечения безопасности в интернете включает функцию защиты онлайн-транзакций, убедитесь, что она активирована.

6. Делайте регулярное резервное копирование своих данных.

7. Установите антивирусную программу. Антивирусные ПО позволяют проверять, обнаруживать и удалять угрозы до того, как они создадут проблему. Оно помогает защитить ваш компьютер и ваши данные от киберпреступников.

8. Периодически обновляйте вашу антивирусную программу, чтобы обеспечить наилучший уровень защиты.

9. Регулярно обновляйте ПО и операционную систему. Постоянное обновление программного обеспечения и операционной системы гарантирует, что для защиты вашего компьютера используются новейшие исправления безопасности.

10. Удалите программное обеспечение, которым вы не пользуетесь.

11. Никогда не подписывайтесь ни на какие компьютерные рассылки.

12. Используйте сильные пароли, которые трудно подобрать, и нигде их не записывайте. Можно воспользоваться услугой надежного менеджера паролей, который облегчит вам задачу, предложив сгенерированный им сильный пароль.

13. Внимательно просматривайте свои банковские выписки [7].

Если вы все-таки стали жертвой интернет-мошенников, то рекомендуется выполнять следующие действия. МВД разработало алгоритм действия для граждан, которые пострадали от действий злоумышленников:

1. Первое действие после того, как вы недосчитались на своем банковском счете некоторой суммы, – это отключить смартфон и вытащить из него сим-карту. Это потенциальное орудие киберпреступления, так что нужно обеспечить его сохранность для сотрудников правоохранительных органов.

2. Далее следует как можно скорее связаться с банком и отозвать денежный перевод, а заодно блокировать все возможные действия с расчетным счетом.

3. Написать заявление в двух экземплярах об отзыве платежа, возврате средств и блокировании доступа к системе «Мобильный банк». Предоставить заявление в банк необходимо в течение одного дня с момента атаки интернет-мошенников.

4. Также необходимо получить в банке детализацию с расчетного счета и обратиться в банк, в который ушли деньги по инициативе злоумышленника, с заявлением о приостановке исполнения платежа и возврате средств.

5. И наконец, написать заявление о факте хищения денежных средств, которое необходимо предъявить в полицию. Для оформления дела понадобится документальное подтверждение хищения денежных средств: выписка из банка, детализация расходов и т. д.

Таким образом, мы сформулировали правила компьютерной безопасности, которые помогут вам не стать жертвами интернет-мошенников. Кроме того, рассмотрели правила поведения в случае, если ваши данные попали в руки злоумышленников. Данные правила и методы применимы ко многим видам киберпреступлений, в частности – к фишингу.

Особенностью схемы фишинга является тот факт, что жертва подобного IT-преступления практически самостоятельно отдает в руки интернет-мошенникам свои данные. Причиной этого может послужить неосторожность или неосведомленность жертвы про подобные схемы преступной деятельности. Итак, сообщения в фишинговой рассылке создаются так, чтобы у получателя не возникло сомнений, что они отправлены из надежного источника, например, от известной компании, которая побуждает человека перейти на поддельный сайт и ввести на нем свои данные, чтобы совершить покупку или оплатить счета. Ничего не подозревая, жертва фишинга вводит свои данные, например, пароли, логины, предоставляет данные банковских карт и т. д. Не просто так данная схема названа фишингом, ведь с английского phishing от fishing переводится как рыбная ловля, выуживание. По аналогии с ловлей рыбы мошенник в роле рыбака рассылает на почту потенциальным жертвам фишинговые ссылки и ждет, пока кто-нибудь из получателей «клюнет» на приманку.

Таким образом, в данной статье мы дали общую характеристику киберпреступности и киберпреступлениям. Выяснили цели и мотивации IT-преступников. Также, мы подробно изучили и раскрыли сущность одной из самых распространенных мошеннических

схем под названием фишинг, показав на конкретных примерах работу данного антисоциального явления. Кроме того, мы выявили причины увеличения количества киберпреступлений. По нашему мнению, ими оказались развитие научно-технического прогресса и пандемия. Киберпреступность является объективным следствием глобализации информационных процессов и появления глобальных компьютерных сетей. С ростом использования информационных технологий в различных сферах деятельности человека растет и использование их в целях совершения преступлений. Возвращаясь к вопросу о фишинге, мы рассмотрели различные методы для борьбы с ним. Как было отмечено выше, самый простой способ защиты от подобного интернет-мошенничесвта заключается в том, чтобы научить людей выявлять фишинг и бороться с ним. Следует подчеркнуть, люди могут самостоятельно снизить угрозу фишинга, просто выполняя действия, представленные в нашей статье. Также, мы обозначили правила компьютерной безопасности и описали алгоритм действий, разработанный МВД для граждан, которые пострадали от действий интернет-мошенников. И, наконец, в данной статье мы охарактеризовали особенности схемы фишинга. По нашему мнению, она заключается в том, что жертва самостоятельно и неосознанно отдает злоумышленникам свои личные данные, такие как пароли, логины и данные от банковских карт.

ЛИТЕРАТУРА

1. *Бородкина Т.Н., Павлюк А.В.* Киберпреступления: понятие, содержание и меры противодействия // Социально-политические науки. – 2018. – № 1. – С. 135-137.
2. *Вестов Ф.А., Шамьенов Н.Р.* Уголовная политика по использованию возможностей цифровых технологий в противодействии мошенничеству // Основы экономики, управления и права. – 2020. – № 6 (25). – С. 53-57.
3. *Дерюгин Р.А.* Киберпреступность в России: современное состояние и Актуальные проблемы // Вестник Уральского юридического института МВД России. – 2019. – № 2. – С. 46-49.
4. *Сторчак С.А.* Обзор антифишинговых технологий // Проблемы науки. –2019. – № 1. – С. 60-64.
5. *Федорович В.Ю.* Что такое «киберпреступление»? // Вестник Московского университета МВД России. – 2020. – № 3. – С. 15-17.
6. Avast. – URL: https://www.avast.ru/c-social-engineering (дата обращения 12.05.2021).
7. Kaspersky. – URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (дата обращения 05.05.2021).

PHISHING AS A THREAT TO THE MODERN INFORMATION SOCIETY

CHERNYSHEVA Anna Vladimirovna
PhD in Philosophy, Associate Professor
SAMOILOV Savva Igorevich
student
N.E. Bauman's Moscow State Technical University
Moscow, Russia

It is difficult for the modern information society to imagine life without interacting with the Internet. However, the information field has not been spared by fraud either. In this article, we will look at one of the types of financially oriented cybercrime called phishing. A feature of this fraudulent scheme is to force the recipient of an email to follow the link on behalf of a legitimate organization in order to obtain the victim's personal data.
Key words: cybercrime, cybercrime, phishing, phishing company, methods of struggle, information.