– сообщение относится к деятельности нанимателя или иным образом происходит в ходе этой деятельности;

– рассматриваемая система предназначена для использования полностью или частично, в связи с этим бизнесом;

– наниматель «предпринял все разумные усилия» для информирования «каждого лица, которое может использовать рассматриваемую телекоммуникационную систему» о том, что сообщения, передаваемые через нее, могут быть прослушаны [1].

Таким образом, установлен четкий перечень случаев, в которых допускается мониторинг коммуникаций без согласия сотрудников. Однако работники, а также в ряде случаев и клиенты нанимателя, должны быть уведомлены о прослушивании или просмотре сообщений, осуществляемых в телекоммуникационной системе нанимателя.

Предлагается внести изменения в Закон «О персональных данных» (далее – Закон) в части трудовых отношений; на данный момент Закон содержит лишь положения о том, что согласие субъекта персональных данных на обработку персональных данных при оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности не требуется в случаях, предусмотренных законодательством. При этом речь идет в том числе и о специальных персональных данных. Предлагается дополнить Закон рядом статей, устанавливающих перечень случаев, когда мониторинг допускается без согласия работников, а также случаев, когда получение согласия необходимо, установить ответственность нанимателей при нарушении прав работников при использовании средств контроля, ограничить возможности использования технических средств критерием «допустимости» в целях ограничения степени «вторжения» нанимателя в личную жизнь работника.

Литература

1. Цифровой контроль за сотрудниками (использование технологий мониторинга на рабочем месте). – Режим доступа: https://xn--h1aax.xn--p1ai/news/tsifrovoy-kontrol-za-sotrudnikami-ispolzovanie-tekhnologiy-monitoringa-na-rabochem-meste/. – Дата доступа: 21.04.2024.
2. Act on the Protection of Privacy in Working Life 759/2004. – Mode of access: https://www.finlex.fi/en/laki/kaannokset/2004/en20040759. – Date of access: 21.04.2024.
3. Bundesdatenschutzgesetz. – Mode of access: https://www.gesetze-im-internet.de/bdsg_2018/. – Date of access: 21.04.2024.
4. Employee monitoring and surveillance: The challenges of digitalization / Eurofound, 2020. – Mode of access: https://www.eurofound.europa. eu/sites/default/files/ef_publication/field_ef_document/ef20008en.pdf. – Date of access: 21.04.2024.

УДК 343

АКТУАЛЬНЫЕ СПОСОБЫ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ В СЕТИ ИНТЕРНЕТ

И. Ю. Тимошенко

Учреждение образования «Гомельский государственный технический университет имени П. О. Сухого», Республика Беларусь

Научный руководитель Д. Н. Лемтюгов

В современном мире Интернет играет ключевую роль в повседневной жизни людей, обеспечивая им доступ к информации, услугам и коммуникации. Однако вместе с возможностями, которые предоставляет Интернет, существует и ряд угроз, включая различные виды мошенничества. Мошенничество в сети Интернет является одной из наиболее распространенных и серьезных угроз, с которыми сталкиваются пользователи. Современные

технологии и возможности сети Интернет предоставляют преступникам новые инструменты и средства для совершения мошеннических действий.

Ключевые слова: Интернет, информация, мошенничество, фишинг, защита данных, кибербезопасность, идентификация.

CURRENT WAYS TO COUNTER FRAUD ON THE INTERNET

I. Y. Timoshenko

Sukhoi State Technical University of Gomel, Republic of Belarus

Science supervisor D. N. Lemtyugov

In the modern world, the Internet plays a key role in people's daily lives, providing them with access to information, services and communication. However, along with the opportunities that the Internet provides, there are also a number of threats, including various types of fraud. Online fraud is one of the most common and serious threats faced by online users. Modern technologies and the capabilities of the Internet provide criminals with new tools and means to commit fraudulent acts.

Keywords: Internet, information, fraud, phishing, data protection, cybersecurity, identification.

В современном законодательстве различные виды мошенничества в сети Интернет рассматриваются как серьезные преступления, и многие страны продолжают совершенствовать законы и меры для борьбы с этими угрозами.

Законы о защите данных и конфиденциальности играют важную роль в предотвращении мошенничества в Интернете. Они определяют правила сбора, хранения и использования личной информации, а также требования к уведомлению об утечках данных и штрафы за нарушения. 15 ноября 2021 г. вступил в силу Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных». Данный правовой акт заложил основы правового регулирования вопросов защиты персональных данных, прав и свобод физических лиц при обработке их персональных данных [1].

Многие страны имеют специальные законы, касающиеся кибермошенничества, которые включают в себя действия, направленные на незаконный доступ к компьютерным системам, взлом, распространение вредоносного программного обеспечения, фишинг и другие виды киберпреступлений. В Уголовном кодексе Республики Беларусь киберпреступления и ответственность за их совершение рассматриваются в Главе 31 «Преступления против компьютерной безопасности» [2].

Законы об электронной коммерции устанавливают правила для онлайн-торговли, защищая права потребителей от мошеннических практик, таких как ложная реклама, обман при онлайн-продажах и неправомерные платежи. В Республике Беларусь одним из основных нормативно-правовых актов в сфере торговли является Закон «О защите прав потребителей» от 9 января 2002 г. № 90-З [3].

Образование и информирование общественности играют ключевую роль в борьбе с интернет-мошенничеством. Осведомленные пользователи сети Интернет способны лучше защитить себя и свои данные от потенциальных угроз.

Одним из мероприятий по информированию общественности является проведение информационных кампаний о сущности и способах защиты от интернет-мошенничества. Примером такой кампании могут служить аудиосообщения в общественном транспорте, описывающие схемы мошенничества и правила безопасности, позволяющие не попасть в мошенническую схему. Этот способ дает возможность охватить большую аудиторию. Также он точечно работает на социально незащищенные слои населения, например, людей преклонного возраста. Эти категории

граждан не так часто пользуются интернетом, поэтому важная информация о мошенниках может попросту не доходить до них. Существует также множество статей в газетах и постов в Интернете, в частности, от МВД, которые также призывают быть внимательным при разговоре с потенциальным мошенником.

Включение темы кибербезопасности в образовательные программы также может помочь в борьбе с мошенничеством в интернете. В вузах, занимающихся подготовкой специалистов в сфере информационных технологий, есть дисциплины, непосредственно связанные с кибербезопасностью. Однако для борьбы с мошенничеством можно приравнять такие дисциплины к общеобразовательным, чтобы произвести максимальный охват среди студентов.

Еще одним эффективным способом профилактики киберпреступлений станет разработка интерактивных ресурсов и материалов, таких как игры, которые помогут пользователям научиться распознавать и избегать угроз интернет-мошенничества:

«Interland» от *Google* – игра помогает детям и подросткам изучить основные аспекты безопасности в Интернете, включая защиту личной информации, распознавание фишинга и установку надежных паролей.

«Anti-Phishing Phil» – это веб-игра, созданная для обучения пользователей распознаванию фишинговых атак. Игроки должны анализировать электронные письма и определять, являются ли они подлинными или фальшивыми.

«Educational Cyber Playground» – это набор образовательных игр и интерактивных упражнений, направленных на обучение детей основам кибербезопасности, включая безопасное поведение в Интернете и защиту личных данных.

Технические средства для борьбы с киберпреступлениями в эпоху активизации интернет-мошенничества стали необходимостью. Сейчас они повсеместно используются: например, сервисы электронной почты и мессенджеров автоматически фильтруют входящие сообщения, идентифицируя и перемещая спам в специальные папки или блокируя его передачу получателям. Механизмы анализа содержания и характеристик сообщений позволяют обнаруживать и блокировать массовые рассылки, фишинговые письма и другие виды нежелательной почты.

Банки также пользуются системами сдерживания атак мошенников на счета клиентов. Такие системы называются «антифрод». Они состоят из набора правил реагирования, которыми руководствуются банки. Система противодействия мошенникам в режиме реального времени проводит анализ данных о платеже (транзакции).

Типовое антифрод-решение в банке состоит из системы обнаружения мошенничества (fraud detection), системы предотвращения мошенничества (fraud prevention) и системы анализа (fraud analysis).

Прекрасным дополнением к способам профилактики интернет-преступлений станет разработка информационных буклетов, инфографики и видеороликов для удобного доступа к ключевой информации. Существует множество видеороликов, в том числе и от банков Республики Беларусь, которые помогают не попасться на мошенников в интернете.

Образование и информирование общественности об интернет-мошенничестве являются основополагающими элементами в обеспечении безопасности в цифровой среде. Чем больше люди осведомлены о возможных угрозах и методах защиты, тем более эффективно можно противостоять мошенничеству в онлайн-мире.

Улучшение законодательства в области борьбы с интернет-мошенничеством играет ключевую роль в предотвращении и пресечении киберпреступлений. Это важное направление в обеспечении безопасности в онлайн-среде, поскольку законы определяют правила и механизмы пресечения преступной деятельности в Ин-

тернете. Нам представляется, что разработка и внедрение отдельной главы в Уголовном кодексе Республики Беларусь, которая бы определила различные формы интернет-мошенничества, такие как фишинг, киберворовство, распространение вредоносных программ и другие киберпреступления, и установила конкретные виды наказаний, являются в нынешних реалиях объективной необходимостью.

Мошенничество в сети Интернет – это серьезная проблема, которая требует внимания со стороны законодательства, правоохранительных органов и общественности. Законы и меры по борьбе с этими угрозами должны быть не только строгими, но и адаптивными, чтобы эффективно противостоять новым формам интернет-мошенничества, которые постоянно появляются в цифровом мире.

Литература

1. О защите персональных данных : Закон Респ. Беларусь от 7 мая 2021 г. 99-З : с изм. и доп. : текст по состоянию на 1 июня 2022 г. – 2024. – Режим доступа: https://etalonline.by/document/?regnum=H12100099. – Дата доступа: 05.05.2024.
2 Уголовный кодекс Республики Беларусь : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : текст Кодекса по состоянию на 9 марта 2023 г. – 2024. – Режим доступа: https://etalonline.by/document/?regnum=hk9900275. – Дата доступа: 03.05.2024.
3. О защите прав потребителей : Закон Респ. Беларусь от 9 янв. 2002 г. 90-З : с изм. и доп. : текст по состоянию на 6 янв. 2024 г. – 2024. – Режим доступа: https://etalonline.by/document/?regnum=H12100099. – Дата доступа: 05.05.2024.

УДК 340

ДЕФОРМИРОВАННОЕ ПРАВОСОЗНАНИЕ: ЗА И ПРОТИВ

И. Д. Цуранова

Учреждение образования «Гомельский государственный технический университет имени П. О. Сухого», Республика Беларусь

Научный руководитель Н. С. Ищенко

Рассмотрено деформированное правосознание, которое искажает, разрушает, трансформирует в худшую сторону позитивные правовые идеи, убеждения, эмоции. Указаны и кратко охарактеризованы различные его формы (правовой нигилизм, идеализм, педантизм, дилетантизм, конформизм, нонконформизм, инфантилизм, прагматизм) и обстоятельства, при которых деформированное правосознание играет положительную роль.

Ключевые слова: деформированное правосознание, нигилизм, идеализм, педантизм, дилетантизм, конформизм, нонконформизм, инфантилизм, прагматизм.

DEFORMED LEGAL AWARENESS: PROS AND CONS

I. D. Tsuranova

Sukhoi State Technical University of Gomel, the Republic of Belarus

Science supervisor N. S. Ishchenko

The article examines the deformed legal consciousness, which distorts, destroys, and transforms positive legal ideas, beliefs, and emotions for the worse. Various forms (legal nihilism; idealism; pedantry; dilettantism; conformism; nonconformism; infantilism; pragmatism) and circumstances in which a deformed sense of justice plays a positive role are indicated and briefly considered.

Keywords: deformed legal consciousness, nihilism, idealism, pedantry, dilettantism, conformism, nonconformism, infantilism, pragmatism.