Приложение 1
к приказу проректора по
идеологической и
воспитательной работе
от «23» 10 2026 № 1006-АКР

ПАМЯТКА
по профилактике преступлений (правонарушений) в сфере информационной безопасности и недопущению хищений

Кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз; сохранение конфиденциальности, целостности и доступности информации в киберпространстве, а также защищенности информационной инфраструктуры.

Киберпреступление – преступления, связанные с использованием компьютерной техники (преступления против информационной безопасности, хищения путем использования средств компьютерной техники, шантаж, вымогательство, изготовление и распространение порнографических материалов и т.д.).

В Уголовном кодексе Республики Беларусь содержится ряд статей, предусматривающих уголовную ответственность за совершение правонарушений и преступлений против собственности и киберпреступления:

ст.ст. 205-219 – правонарушения и преступления против собственности;

ст. 209 «Мошенничество»;

ст.212 «Хищение имущества путем модификации компьютерной информации»;

ст.349 «Несанкционированный доступ к компьютерной информации»;

ст.350 «Уничтожение, блокирование или модификация компьютерной информации»;

ст.352 «Неправомерное завладение компьютерной информацией»;

ст.354 «Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств»;

ст.355 «Нарушение правил эксплуатации компьютерной системы или сети»

Основными формами обмана являются телефонное и интернет-мошенничество, а также фишинговые ресурсы.

ФИШИНГ (англ. phishing от fishing «рыбная ловля, выуживание») – вид мошенничества, цель которого является получение конфиденциальных данных для доступа к различным сервисам (электронной почте, странице в социальной сети, интернет-банкингу и т.д.).

С целью получения личных данных владельцев счетов мошенники создают страницы-клоны сайтов банков, театров, кальянных и инвестиционных (торговых) бирж.

ДЛЯ ПРЕДОТВРАЩЕНИЯ ПОДОБНОГО НЕОБХОДИМО:

задуматься о причинах низкой цены на товар, отличающейся от цены за тот же товар на сайте или насторожиться почему у магазина на сайте указаны другие цены;

тщательно проверять информацию о магазине: связаться с продавцом по белорусскому номеру по мобильной связи, а не через Интернет;

использовать отдельную карту для расчетов в сети Интернет;

не переходить по ссылкам от неизвестных вам лиц;

проверять адрес страницы, где вводите данные карты (для белорусских организаций в адресной строке должно быть так: «название сайта».BY/«раздел сайта»);

подключить (проверить подключение) в настройках карты бесплатную услугу от банка «3-D Secure» – это дополнительная защита от банка, которая предлагает ввести код, пришедший в смс-сообщении.

ВИШИНГ (англ. vishing – voice + phishing) – это устная разновидность фишинга, при которой злоумышленники посредством телефонной связи, используя приемы, методы и технологии социальной инженерии, под разными предлогами, искусно играя определенную роль (как правило, сотрудника банка, технического специалиста и т.д.), вынуждают человека сообщить им свои конфиденциальные банковские или персональные данные либо стимулируют к совершению определенных действий со своим банковским счетом или банковской картой.

Мошенники под видом работников банка, операторов связи или государственных органов обращаются к гражданам, создают стрессовую ситуацию, сообщают о проблеме, а потом предлагают помощь в ее решении. При этом, чтобы войти в доверие, могут выслать фото служебных документов или даже выйти на видеосвязь в мессенджере.

Распространен способ, когда мошенники, используя различные вымышленные ситуации, убеждают потенциальных жертв загрузить направленный в мессенджере файл или установить определенное мобильное приложение. В обоих случаях мошенники получают возможность удаленно управлять устройством, на котором установлено.

Таким образом, они получают доступ к личным данным пользователей, в том числе имеют возможность оформить онлайн-кредит. Также злоумышленники убеждают оформить кредиты в банках, а деньги перевести на «защищенный» счет.

Всегда надо быть начеку и не доверять незнакомым, ни под каким предлогом не устанавливать непроверенные программы и файлы, полученные в мессенджере от неизвестных, не передавать кому бы то ни было деньги и не переводить их на банковские счета по указанию незнакомых!

Мошенники для совершения преступлений изучают свою жертву, собирают в сети Интернет данные о ней и ее интересах, окружении и прочем. Имея образец голоса или фото знакомых, могут создавать фейковые текстовые или видеосообщения.

Публичность, доступность и анонимность – благоприятная почва для киберпреступности!

Чтобы не стать жертвой киберпреступника, как можно раньше закончите разговор с неизвестным лицом, кем бы он не представился.

ИНВЕСТИЦИОННЫЕ ПЛАТФОРМЫ

В сети Интернет размещают рекламу якобы инвестиционных платформ, которых на самом деле не существует, чтобы заманить вкладчиков и похитить их деньги. Первым шагом для связи с куратором является заполнение формы, где необходимо оставить свои имя и телефон. Далее с заинтересовавшимся связывается так называемый куратор, под руководством которого в надежде заработать легкие деньги потенциальная жертва сама переводит деньги на электронный кошелек. Чтобы получить хотя бы вложенные деньги обратно, мошенники требуют заплатить комиссии, взносы и т.д. Некоторое время мошенники рисуют жертве прибыль, пока у обманутого человека не закончатся деньги, потом связь с ним прекращается. Деньги остаются на счетах мошенников.

ФЕЙКОВЫЕ МАГАЗИНЫ в соцсетях

Мошенники намеренно создают аккаунты от имени магазинов, в которых размещают объявления несуществующих товаров с заниженными ценами (обувь, одежда, мобильные телефоны, постельное белье, автомобильные шины, новогодние ели, садовые кресла-качалки-коконы и другие товары). Потенциальный покупатель связывается с администратором «магазина» и обещает доставить товар после частичной или полной оплаты. Перевод денег предлагают произвести на банковскую карту или на счет через ЕРИП, что притупляет бдительность. После получения денежных средств, Интернет-магазин товар не высылает, а покупателя блокирует.

СВАТИНГ

В молодежной игровой киберсреде распространяется тренд под названием «сватинг». Его суть заключается в том, чтобы создать неблагоприятную обстановку госорганам, нарушить режим их работы, или отомстить своему обидчику, создав для него проблемы с правоохранительными органами. Чаще всего установленные лица – несовершеннолетние.

Подростки интересовались темой сватинга и в большинстве случаев знали, что за совершение данных деяний уголовная ответственность наступает с 14 лет и предусматривает наказание вплоть до 7 лет лишения свободы.

ВОВЛЕЧЕНИЕ В КИБЕРПРЕСТУПНОСТЬ

Для получения за границей похищенных денег, а также для запутывания «цифровых следов» мошенникам необходимо перевести их через

промежуточные счета, открытые в белорусских банках на подставных лиц, так называемых «дропов». Часто промежуточных счетов бывает более десятка. В Республике Беларусь открыть банковский счет может дееспособный гражданин с 14 лет, то есть даже несовершеннолетние могут открыть банковские счета. Этим в своих целях пользуются преступники. Находясь за границей, злоумышленники подбирают лиц, которые согласятся открыть банковский счет на свое имя и продать за небольшую сумму реквизиты доступа к нему – это логины и пароли для входа в личный кабинет в Интернет-банкинге, а также предоставить разовый смс-код или карту кодов.

Напрямую мошенники в Интернете не могут размещать объявления о поиске таких лиц, поэтому свой интерес они прикрывают предложением различного другого заработка, не вызывающего подозрения. Чаще всего отзываются на такие вакансии лица с нестабильным или небольшим доходом, в большинстве – молодежь. Сначала инициатор объявления разочаровывает заинтересовавшегося подработкой, сообщает, что данная вакансия уже закрыта, и тут же предлагает иной вид заработка, например, оформить банковский счет и передать за вознаграждение данные для доступа к нему.

Кроме похищенных киберпреступниками денег по промежуточным счетам также могут проводиться деньги, полученные от незаконного оборота наркотиков. Ответственность за происхождение прошедших по банковским счетам денег несут владельцы таких счетов.

Надо знать, что в законодательстве Республики Беларусь статьей 222 Уголовного кодекса предусмотрена ответственность вплоть до 10 лет лишения свободы за изготовление в целях сбыта либо сбыт банковских платежных карт или иных платежных инструментов, таких как банковские счета или электронные кошельки, а также распространение данных доступа к ним. Имеются факты, когда в преступную деятельность были вовлечены несовершеннолетние.

За совершение сделок с криптовалютой в пользу третьих лиц грозит крупный штраф и обращение в доход государства до ста процентов суммы дохода, полученного в результате такой деятельности.

ОПЕРАЦИИ С КРИПТОВАЛЮТОЙ

Указом Президента Республики Беларусь от 17 сентября 2024 г. № 367 «Об обращении цифровых знаков (токенов)» (далее – Указ № 367) установлена обязанность для физических лиц совершать операции по покупке-продаже криптовалюты за денежные средства (белорусские рубли, иностранную валюту или электронные деньги) только у криптобирж (операторов обмена криптовалют), являющихся резидентами Парка высоких технологий, а также перечислять (переводить) денежные средства со своих банковских счетов, электронных кошельков исключительно указанным резидентам ПВТ. Совершение операций по купле (продаже) криптовалюты на иностранных криптобиржах и у физических лиц является незаконным и запрещается.

Разрешено: покупать токены (криптовалюту) за денежные средства только на белорусских криптобиржах, являющихся резидентами Парка высоких

технологий; обменивать токены на другие токены на любых криптоплатформах без ограничений, например, обменивать Bitcoin на Ethereum.

Запрещено: покупать или продавать токены (криптовалюту) за денежные средства на иностранных криптобиржах.

Наиболее распространенные способы хищения имущества путем модификации компьютерной информации и типичные последствия их применения.

1. Обман потерпевшего под предлогом продажи вещей на интернет-площадке. На торговых интернет-площадках правонарушитель находит объявление, размещенное пользователем о продаже какого-либо имущества, после чего в различных мессенджерах пишет данному пользователю о том, что хочет приобрести его имущество, указанное в объявлении, однако по различным причинам не имеет возможности лично за ним приехать. Он предлагает произвести оплату путем перевода денежных средств на банковскую платежную карточку (далее - БПК) пользователя и после того, как он соглашается, высылает в его адрес ссылку с фишинговой (поддельной) страницей сайта определенного банковского или иного учреждения (страница может быть визуально схожа со страницей интернет-банкинга и отличаться только символом в адресной строке доменного имени сайта). Переходя по указанной ссылке, пользователь не замечает, что находится на поддельной странице интернет-банкинга. В открывшемся окне на указанном сайте пользователю, как правило, предлагается ввести свои реквизиты БПК, логин и пароль от интернет-банкинга либо паспортные данные, а также код из смс-сообщения. После ввода указанной информации пользователю сообщается об ошибке либо невозможности совершить платеж. В это время всю введенную информацию видит злоумышленник и вводит на действительном сайте банка или ином ресурсе, получая тем самым доступ к денежным средствам жертвы и совершая их хищение. Проведя несанкционированную операцию по переводу денежных средств, правонарушитель нередко сообщает пользователю, что по техническим причинам не может ее осуществить, и просит повторить действия с какой-то другой карточкой (родственников или знакомых).

2. Обман поперевшего под предлогом покупки вещей на интернет-площадке. На торговых интернет-площадках злоумышленник размещает объявление о продаже какого-либо имущества, пользующегося спросом, и преднамеренно устанавливает цену ниже рыночной. Пользователи, увидевшие указанное объявление, пишут лицу, его разместившему, и в ходе переписки злоумышленник сообщает, что не имеет возможности лично встретиться для передачи имущества, предлагает воспользоваться курьерскими услугами (например, «Доставка Куфар», «Белпочта (ЕМС)», «Курьерская служба (СДЭК)»). При согласии покупателя правонарушитель высылает в адрес пользователя ссылку с фишинговой страницей сайта како-го-либо вида доставки, где предлагается ввести реквизиты БПК для оплаты товара, услуг курьера, паспортные данные, номер мобильного телефона, а также код из смс-сообщения. После ввода данной информации пользователю обычно сообщается об ошибке либо сайт перестает загружаться («зависает»). В это время всю

введенную информацию видит злоумышленник и вводит ее на действительном сайте банка, получая доступ к денежным средствам пользователя и совершая их хищение. Проведя несанкционированную операцию по переводу денежных средств, он сообщает пользователю, что по техническим причинам не может ее осуществить, и просит повторить указанные действия с какой-то другой карточкой (родственников или знакомых).

3. Обман потерпевшего под предлогом оказания помощи от имени банковских работников. На мобильный телефон потерпевшего поступает входящий звонок от злоумышленника. Как правило, при этом последний пользуется сервисом по подмену номера телефона и указывает абонентский номер, принадлежащий какому-либо банку или схожий с ним, либо использует для осуществления звонка мессенджер (например, Viber), где у вызывающего абонента имеется ярлык с логотипом банковского учреждения. Далее он представляется сотрудником банка (может назвать пользователя по имени и отчеству, а также сообщить часть номера БПК либо информацию о недавно совершенных оплатах). Злоумышленник сообщает о подозрительных операциях по переводу денежных средств в крупных суммах на карт-счета иностранных банков или оформлении кредитов на имя потерпевшего. Когда потерпевший отвечает, что никаких операций он не производил, злоумышленник сообщает, что указанные операции необходимо заблокировать, в связи с чем просит пользователя назвать отдельные реквизиты БПК либо паспортные данные и сообщает, что высылает в адрес пользователя смс-сообщение с кодом, который необходимо назвать после звукового сигнала. В это время все полученные сведения злоумышленник вводит на сайте банка, получает доступ к денежным средствам пользователя и совершает их хищение. Следует помнить, что запрашиваемая преступником информация сотрудникам банка не требуется ни при каких обстоятельствах и они не будут узнавать о ней у клиента.

4. Обман потерпевшего под предлогом покупки билетов в кино, театр, бронирования кальянных, саун и пр. (так называемая схема «Антикино»). Киберпреступники с фейковых аккаунтов на различных сайтах, представляясь девушками, знакомятся с мужчинами и предлагают продолжить общение в мессенджерах. Для убедительности они направляют собеседникам фотографии и голосовые сообщения, ведут беседы по телефону. Затем мошенники присылают фишинговую ссылку на сайт, например, несуществующего кинотеатра, в котором предлагают провести время. Мужчинам необходимо забронировать места и все оплатить. Потерпевшие вводят реквизиты своих БПК, тем самым предоставляя мошенникам полный контроль над карт-счетами. Таким образом злоумышленники завладевают деньгами. При попытке обратиться в службу поддержки сайта обманутые граждане снова попадают на киберпреступников, что препятствует своевременному обращению в правоохранительные органы.

5. Обман потерпевшего под предлогом продления срока действия SIMкарты. На телефон поступает звонок от неизвестного, представляющегося официальным лицом сотовой компании, которое сообщает об окончании срока действия SIM-карты. Для его продления мошенники просят назвать код из смссообщения, который приходит на телефон. Так они пытаются получить

доступ в личный кабинет на сайте оператора связи, после чего устанавливают переадресацию на контролируемый преступниками номер. Иногда для вхождения к ним в доверие предлагают перейти потерпевшим по фейковой ссылке.

6. Обман потерпевшего под предлогом оказания содействия в получении посылки на «Белпочте». Потерпевшему направляются сообщения о пришедшей посылке, которую можно получить после заполнения недостающей информации, перейдя по ссылке. В реальности же последняя является фишинговой, а ввод данных позволяет мошенникам получить доступ к карт-счету и похитить деньги.

7. Обман потерпевшего под предлогом оказания помощи его родственнику или близкому. На мобильный телефон потерпевшего поступает входящий звонок от злоумышленника, который сообщает, что родственник жертвы попал в неприятную историю (например, он участник ДТП, ему грозит тюрьма, он находиться в больнице). После этого трубку берет якобы врач (следователь, милиционер, прокурор) и говорит, что срочно нужны деньги, чтобы оплатить дорогостоящее лечение или дать взятку («откупиться»). В процессе диалога потерпевший беспрекословно выполняет требования мошенника: в некоторых случаях устанавливает на своем телефоне программу AnyDesk, RustDesk, с помощью которых мошенник отслеживает и контролирует все его действия, выведывает конфиденциальную информацию доступа к банковскому счету, вынуждает оформить и переоформить кредит либо сообщает, что приедет курьер, которому следует передать наличные деньги. Таким образом, в результате мошеннических действий потерпевший лишается денежных средств.

8. Обман потерпевшего под предлогом временного заимствования денег. После несанкционированного доступа к страницам пользователя в социальных сетях злоумышленник рассылает от его имени лицам, находящимся в разделе «Друзья», сообщения с просьбой об оказании помощи, выражающейся в переводе денежных средств, для чего используются различные предлоги: «Привет, не мог бы ты одолжить мне денег? Отдам через пару дней», «Привет, положи, пожалуйста, 10 рублей на телефон, я отдам», «Привет, можно я переведу тебе на карту свои деньги, а то у меня закончился срок действия карты (или не получается перевести на свою)?». Далее преступник входит в доверие к неравнодушным пользователям и якобы для перевода денежных средств просит сообщить реквизиты БПК и коды из смс-сообщений. Пользователь, введенный в заблуждение относительно лица, осуществившего указанную рассылку, не догадавшийся о преступности его намерений, сообщает запрашиваемые сведения, ввиду чего злоумышленник получает доступ к денежным средствам жертвы и совершает их хищение. Проведя несанкционированную операцию по переводу денежных средств, то есть фактически уже похитив деньги с одной карты, злоумышленник часто сообщает, что по техническим причинам не может осуществить операцию и просит повторить указанные действия с какой-либо другой карточкой (родственников или знакомых), чтобы продолжить хищения с других банковских счетов. Все приведенные примеры показывают, что мошенники используют фактор неожиданности и создают для жертвы

максимально неудобные, ограниченные по времени условия для анализа происходящего. Обычно их интересует номер БПК, логин и пароль от кабинета пользователя, коды из смссообщения.

Для того чтобы обезопасить себя и свои денежные средства, необходимо соблюдать следующие правила:

не разглашать логины, номера телефонов, пароли, ПИН-коды, реквизиты БПК, расчетных счетов, секретные (CVC/CVV-коды, данные касательно последних платежей и срока действия пластиковых карточек третьим лицам;

подключить и использовать технологию «3D Secure», которая обеспечивает безопасность платежей в сети Интернет, позволяет однозначно идентифицировать подлинность держателя карты, осуществляющего операцию, и максимально снизить риск мошенничества. При использовании этой технологии держатель БПК подтверждает каждую операцию по своей карточке специальным сеансовым паролем, который он получает в виде смс-сообщения на свой мобильный телефон;

исключить передачу посторонним лицам полученных в смс-сообщениях сеансовых паролей для подтверждения операций, а также своих БПК, каким бы то ни было способом;

вводить секретные данные только на сайтах, защищенных сертификатами безопасности и механизмами шифрования. Доменные имена этих ресурсов в адресной строке каждого браузера начинаются с https://, а не http. //;

производить регулярный мониторинг выполненных операций, используя раздел с историей платежей, контролировать свои списания:

использовать дополнительный уровень безопасности (системы многоуровневой аутентификации, смс-информирование о расходных операциях);

подобрать сложный пароль, используя набор цифр, заглавных и строчных букв, который будет понятен лишь владельцу аккаунта. Изменять пароль каждые 2-4 недели, если пользуетесь чужими компьютерами для входа в систему интернет-банкинга;

не применять автоматическое запоминание паролей в браузере, если к персональному компьютеру открыт доступ посторонним лицам или если для входа на сайт используется компьютер общего доступа;

устанавливать антивирусную защиту, своевременно обновляя базы данных вирусов и шпионских утилит;

привязать к MAC или IP-адресу вход в личный кабинет на сайте интернетбанкинга;

выкладывать фотографию БПК в сеть Интернет, поскольку имеющихся на изображении сведений может быть достаточно для совершения операций с использованием этих данных без ведома владельца.

Не попадитесь на уловки мошенников!

Помните:

Представители правоохранительных органов, государственных организаций НИКОГДА НЕ ЗВОНЯТ на МЕССЕНДЖЕРЫ! (исключения, если Вы сами дали свой номер для связи сотруднику и знаете его лично);

ни под каким предлогом не сообщайте по телефону персональные (паспортные) данные, номера банковских карт или одноразовые пароли, пришедшие Вам на мобильный телефон;

приложение мобильного оператора можно скачивать только из магазинов «Google Play», «App Store», «App Gallery», а не с направленных Вам ссылок на сайты незнакомыми лицами;

никогда не оформляйте кредиты по просьбе или требованию третьих - не проводите через банкоматы, а также системы банковского обслуживания сети Интернет, никакие денежные операции по инструкциям, полученным по телефону или мессенджеру.

Если поступил сомнительный звонок, незамедлительно завершите разговор и обратитесь в милицию по номеру «102».

КАК ОТСЕЧЬ ЗВОНКИ МОШЕННИКОВ: ПРОСТАЯ ИНСТРУКЦИЯ

Защитите себя, настроив популярные мессенджеры так, чтобы звонить вам могли ТОЛЬКО люди из вашей телефонной книги.

Это займет меньше минуты!

📱 В Viber:

Откройте Viber →

вкладка «Ещё» (внизу справа)→

⚙ □ Настройки →

💬 Вызовы и сообщения.

Включите опцию ☑ «Защита от лишних звонков».

📱 В Telegram:

Откройте Telegram → «Настройки» (шестеренка в меню) →

Конфиденциальность → Звонки →

«Кто может звонить мне?».

Выберите вариант «Контакты».

📱 В WhatsApp:

Откройте WhatsApp → вкладка «⋮» (три точки, Android) или «Настройки» (iOS) → Конфиденциальность → Вызовы.

Активируйте опцию «Тихие вызовы от неизвестных».

Помните:

1. Официальные структуры НИКОГДА не запрашивают по телефону коды из СМС, CVV-коды карт, пароли от интернет-банка или предложат установить посторонние программы.
2. Банки НЕ БЛОКИРУЮТ карты, предварительно не уведомив клиента через официальное приложение банка или СМС на короткий номер банка (который всегда одинаков и указан на обороте карты).
3. Любой звонок о проблемах с родственником ТРЕБУЕТ ПЕРЕПРОВЕРКИ. Немедленно положите трубку и самостоятельно позвоните родным или их близким знакомым по известным вам номерам.

Если вы пострадали от мошенничества:

1. Немедленно позвоните в свой банк по официальному номеру (с сайта или оборота карты), чтобы заблокировать карту (если сообщали реквизиты или коды).
2. Позвоните в межбанковскую систему идентификации по короткому номеру – 141! (заблокируют переводы ваших денежных средств).
3. Немедленно сообщите о происшествии в милицию по телефону 102! Чем быстрее вы обратитесь, тем выше шансы задержать преступников.

Будьте бдительны! Эти знания помогут спасти Ваши деньги!