

## **Информационный материала на тему: «Обеспечение безопасности в сфере информационных технологий»**

Справочно:

- количество интернет-пользователей в мире оценивается в 4,021 млрд. (данные приводятся в отчете международного агентства «We are Social», специализирующегося на исследованиях в области социальных медиа);

- по данным «Белстата» на начало 2017 года в Беларуси насчитывается 11,083 миллиона абонентов сети Интернет (2016 – 10,3), большинство пользователей сети в возрасте от 25 до 54 лет (58,1%), 68,3% абонентов выходят в сеть Интернет ежедневно;

- совокупная абонентская база операторов мобильной связи составляет около 11,5 миллионов абонентов, на 1000 человек приходится 1205 абонентов (один человек может быть «дважды абонентом») при охвате территории республики 98,1%, большая часть пользуется услугой передачи данных;

- продолжается внедрение в повседневную жизнь электронных платежных средств. По данным Нацбанка, банками Беларуси по состоянию на 1 января 2018 года эмитировано 13 854 900 карт;

- постоянно растет количество интернет-магазинов (рост за пять лет в 35,5 раза, 2017 год – более 15 тысяч зарегистрированных);

Такое развитие электронных технологий и телекоммуникационных сетей, всеобщая доступность сети Интернет наряду с положительными моментами создают и предпосылки к активному проявлению противоправных действий в данной сфере.

В целом по республике отмечается рост выявленных высокотехнологичных преступлений (+25,4%, с 2471 в 2016 до 3099 в 2017). Более двух третей преступлений (74,8%), выявленных в сфере высоких технологий, относятся к хищениям путем использования компьютерной техники (ст.212 УК РБ). Увеличилось количество выявленных преступлений против информационной безопасности (ст.ст. 349-355 УК РБ). Указанные обстоятельства в первую очередь обусловлены ростом числа выявленных фактов неправомерного завладения компьютерной информацией (в 2,2 раза, с 13 до 29), модификацией компьютерной информации (+92,3%, с 13 до 25) и несанкционированного доступа к компьютерной информации (+79,1%, с 258 до 462).

В 2017 году установлено 1052 лица (2016г. - 966), виновных в совершении высокотехнологичных преступлений. К уголовной ответственности привлечено 956 (2016 г. - 866) человек, в т.ч. 294 (2016 г. -

286), имеющих судимость, 683 (2016г. -648) неработающих и неучащихся и 34 (2016г. - 34) несовершеннолетних (за совершение хищения путем использования компьютерной техники уголовная ответственность предусмотрена с 14 лет, изменения в уголовный кодекс внесены Законом Республики Беларусь от 5 января 2016 года №356-З и начали действовать с 4 апреля 2016 года).

Количество обращений граждан в ОВД области по фактам противоправной деятельности с использованием сети Интернет и компьютерных технологий постоянно увеличивается. Граждане обращаются в ОВД с заявлениями по фактам несанкционированного доступа к их Интернет ресурсам (анкетам в социальных сетях, электронным почтовым ящикам, электронным кошелькам), мошеннических действий в сети Интернет, противоправного использования реквизитов доступа к сети Интернет, умышленного уничтожения и блокировки компьютерной информации и др. За первый квартал текущего года таких заявлений поступило 164 (2017г. - 67).

Остановимся на наиболее распространенных случаях, когда наши граждане становятся жертвами противоправных действий, совершенных с использованием компьютерных технологий и сети Интернет, а также на том, что нужно делать, чтобы предупредить наступление негативных последствий.

Чаще всего мы страдаем от так называемых Интернет – мошенничеств, причем большая их часть связана с покупками с использованием сети Интернет. Наши граждане на различных интернет-ресурсах находят объявления о продаже интересующих их вещей, и затем переводят «продавцам» значительные суммы денег, в результате лишаясь и денег и не получая купленного товара. Надо учесть, что когда Вы покупаете что-либо в магазине, Вы видите то, что покупаете и того, кто продает. Покупая в Интернете, Вы фактически не видите товар, а формируете представление о нем по картинке, видеоролику или просто по описанию продавца. Кроме того, продавец может оказаться не тем, за кого себя выдает. В связи с чем, опасайтесь покупать в сети Интернет товар, цена на который явно занижена, всегда имейте ввиду, что рассчитываясь за покупку, произведенную с использованием сети Интернет, вы в определенной мере рискуете остаться без денег и без покупки. Особенно это касается случаев, когда покупка осуществляется через социальные сети, так называемые интернет-барахолки, аукционы и из-за границы. В случае, если Вы попали на мошенников и оплатили товар отправив деньги за границу, привлечь их к ответственности и вернуть Ваши деньги, будем откровенны, практически невозможно.

Не даром гласит народная мудрость «бесплатный сыр только в мышеловке». Если к Вам на электронный почтовый ящик или на мобильный телефон пришло сообщение, о том, что:

- Вы выиграли крупную сумму денег или дорогостоящую вещь в лотерею, в которую не играли, и для того, чтобы получить выигрыш, с Вас требуют некоторую сумму денег,

- у Вас за границей нашелся богатый родственник, который оставил Вам огромное наследство, и для оформления документов на его получение с Вас просят деньги,

- дорогостоящий мобильный телефон или даже автомобиль продается за пол цены, весьма срочно и деньги нужно направить за пределы страны, - **остерегайтесь, это – мошенничество!**

В настоящее время в сети Интернет существует много сервисов, позволяющих оплачивать различные услуги или просто переводить денежные средства с абонентских счетов сотовых операторов, чем в последнее время также часто пользуются мошенники. Это так называемые sms-мошенничества. Мошенник под различными предложениями пытается узнать у жертвы абонентский номер сотового телефона, а также пришедший в последствие на данный номер код. Этого достаточно для того, что бы денежные средства с абонентского счета жертвы перетекли на счета мошенника. Получая доступ к абонентскому счету, злоумышленник завладевает денежными средствами абонента. Зачастую необходимую информацию преступники получают при знакомствах в социальных сетях, нередко обманывая несовершеннолетних. Пример: молодая девушка 13 лет знакомится в социальной сети «ВКонтакте» якобы с «парнем», который после некоторого общения узнает номер ее мобильного телефона, а позже просит сообщить содержание sms-сообщения, пришедшего на данный номер, где указывается код для проведения операций с абонентским счетом. Через некоторое время с лицевого счета абонента списывается значительная сумма денег, а анкета «парня» в социальной сети исчезает.

Если кто-то из Ваших знакомых в социальной сети или через программу «Skype» просит Вас срочно перечислить денежные средства на абонентский номер или электронный кошелек, предоставить сведения о своей банковской платежной карточке (чаще всего фотографии лицевой и оборотной стороны карточки), прежде чем выполнить просьбу, постарайтесь связаться с ним по телефону и уточнить действительно ли это он. Анкета Вашего знакомого может быть взломана, и от имени знакомого Вам может писать мошенник.

Если Вам на электронный ящик поступило сообщение от незнакомого человека или организации, будьте благоразумны и не старайтесь открыть прикрепленный к письму файл не смотря на предупреждения антивирусной программы о том, что это опасно, и это может навредить Вашему

компьютеру. Прикрепленный файл может быть опасным вирусом, который может уничтожить данные на Вашем компьютере.

Если Вы ищете в сети Интернет какие-то бесплатные программы, фильмы, музыкальные композиции, имейте в виду, что под видом так называемой «халявы» Вам обязательно постараются подсунуть вирус или как минимум платную услугу, о подключении которой Вы можете сразу и не узнать.

**Помните, разместить в сети Интернет для общего доступа информацию о себе, свои фотографии, это тоже самое, что разместить их на доске объявлений на остановке общественного транспорта.**

Если Вы уже стали активными пользователями сети Интернет, надо стараться повышать свой уровень компьютерной грамотности, принимать соответствующие меры безопасности, а именно устанавливать на своем компьютере и постоянно обновлять антивирусное программное обеспечение, не заходить на подозрительные сайты и подозрительные ссылки. Любой, незаметно полученный Вами, компьютерный вирус может стать для Вас серьезной проблемой. Так, например, в текущем году десятки наших граждан пользователей сети Интернет при просмотре различных сайтов сети Интернет неожиданно для себя обнаруживали, что работа компьютера заблокирована, а на экран монитора выводится сообщение о блокировке компьютера за просмотр и распространение порнографических материалов, и для получения кода для разблокировки необходимо заплатить штраф на указанные в сообщении электронные кошельки и абонентские номера сотовых операторов. Это следствие работы вредоносной программы, так называемого «вируса-вымогателя». Естественно заплатив деньги, никакого кода разблокировки Вы не получите, а только пополните счет преступников. В таких случаях надо обратиться к специалистам, чтобы они «вылечили» ваш компьютер. Помните, что милиция в нашей стране не берет штрафы путем перечисления денежных средств на электронные кошельки или абонентские номера сотовых операторов. Да и просмотр порнографических материалов у нас не наказуем.

В области основную работу по противодействию киберпреступности выполняет специализированное подразделение по раскрытию преступлений в сфере высоких технологий.

Дополнительную информацию Вы можете получить на сайте УВД Брестского облисполкома, а в случае возникновения каких-либо вопросов, связанных с преступлениями в сфере высоких технологий Вы можете позвонить по указанным телефонам:

начальник отдела:	(80162) 200203
сотрудники	(80162) 210769
	(80162) 275517