**УО «МОЛОДЕЧНЕНСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ ИМ. И.В.ЗАЛУЦКОГО»**

**ПАМЯТКА ДЛЯ УЧАЩИХСЯ**

**ПРОФИЛАКТИКА И ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ**

**КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПЛЕНИЯ?**

**ОТВЕТСТВЕННОСТЬ ПО КИБЕРПРЕСТУПЛЕНИЯМ**



**ПРОФИЛАКТИКА И ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ**

Киберпреступность является новой и одной из быстроразвивающихся формой транснациональной преступности. Сеть Интернет стала практически незаменимым средством повседневной связи и обмена информацией по всему миру, и преступники не могут этим не пользоваться. Два миллиарда пользователей Интернета по всему миру создают идеальную среду для совершения преступлений, где можно действовать анонимно и получать доступ к любой персональной информации, которую мы, желая того или нет, размещаем в сети. В последние годы безопасность в сети Интернет подвергается более серьезным угрозам, и от преступлений в глобальном киберпространстве страдают более 431 миллиона взрослых пользователей.

**Что такое киберпреступление**

В настоящее время при характеристике компьютерных преступлений используется целый ряд понятий: «информационное преступление», «киберпреступление», «преступление в сфере компьютерной информации», «преступление в сфере высоких технологий», «виртуальное преступление».

Согласно действующему законодательству Республики Беларусь, в содержание понятия «компьютерная преступность» включают:

1) преступления против информационной безопасности (модификация компьютерной информации, несанкционированный доступ к компьютерной информации, компьютерный саботаж, неправомерное завладение компьютерной информацией, разработка, использование либо распространение вредоносных программ, нарушение правил эксплуатации компьютерной системы или сети и др.);

2) хищения путем использования средств компьютерной техники;

3) изготовление и распространение порнографических материалов или предметов порнографического характера, в том числе с изображением несовершеннолетнего;

4) иные преступления, так или иначе связанные с использованием компьютерной техники: доведение до самоубийства путем систематического унижения личного достоинства через распространение каких-либо сведений в сети Интернет; разглашение врачебной тайны; незаконное собирание либо распространение информации о частной жизни; клевета; оскорбление; распространение ложной информации о товарах и услугах; заведомо ложное сообщение об опасности; шпионаж; умышленное либо по неосторожности разглашение государственной тайны; умышленное разглашение служебной тайны и др.

Таким образом, к **компьютерным преступлениям** относятся правонарушения, при совершении которых средства компьютерной техники выступают как орудия совершения преступления либо как предмет преступного посягательства.

Вишинг — один из методов мошенничества, злоумышленники используя телефонную коммуникацию и играя определённую роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определённых действий со своим карточным счетом / платежной картой.

Фишинг – техника «социальной инженерии», направленная на получение конфиденциальной информации. Обычно злоумышленник посылает потерпевшему e-mail, подделанный под официальное письмо – от банка или платежной системы – требующее «проверки» определенной информации, или совершения определенных действий. Это письмо, как правило, содержит ссылку на фальшивую веб-страницу, имитирующую официальную, с корпоративным логотипом и содержимым, и содержащую форму, требующую ввести необходимую для преступников информацию – от домашнего адреса до пин-кода банковской карты.

Сваттинг — тактика домогательства, которая реализуется посредством направления ложного вызова той или иной службе. Например, люди сообщают о минированиях, преследуя цель устроить неразбериху и панику в конкретном месте.

Смишинг – вид мошенничества (англ. smishing – SMS + phishing), целью которого является переход по ссылке из SMS и/или загрузки вредоносного программного обеспечения. Смишинг-сообщение обычно имеет схожий внешний вид сообщения от банка, государственного учреждения, оператора электросвязи, известного магазина, а также о внезапном выигрыше в лотерею или акции и т.д

Мошенничество в виде лотереи – это электронное сообщение, информирующее вас о том, что вы выиграли огромную сумму денег, и для того, чтобы получить свой приз или выигрыш, вам нужно заплатить небольшую плату.

Как правило, подобные методы применяются мошенниками для кражи данных кредитных карт и денежных средств. Кроме того, через Интернет все чаще совершаются преступления, связанные с нарушением авторских прав и прав интеллектуальной собственности, а также распространением материалов с детской порнографией и сценами насилия.



**КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПЛЕНИЯ?**

Для создания препятствий правоохранительным органам для раскрытия подобных преступлений злоумышленники: меняют сотовые телефоны, места своего нахождения; оформляют сим-карты и открывают счета в банках на подставных лиц; используют анонимные электронные кошельки и предоплаченные банковские карты, Proxy-серверы и различные программы, скрывающие фактические IP-адрес и место нахождения, привлекают лиц, не осведомленных о противоправности их действий, применяют другие способы конспирации. Это касается не только хищений, но и преступлений в сфере компьютерной информации. При этом данные преступления носят скоротечный, многоэпизодный (серийный), и трансграничный характер.

1. **Никогда, никому и ни при каких обстоятельствах не сообщать реквизиты своих банковских счетов и банковских карт**, в том числе лицам, представившимся сотрудниками банка или правоохранительных органов, при отсутствии возможности достоверно убедиться, что эти люди те, за кого себя выдают.

В случае поступления звонка «от сотрудника банка» необходимо уточнить его фамилию, номер телефона, после чего завершить разговор и самим позвонить в банк.

Необходимо принимать во внимание, что реальному сотруднику банка известна следующая информация: фамилия держателя карты, паспортные данные, какие карты оформлены, остаток на счете.

Не следует сообщать в телефонных разговорах (даже сотруднику банка), а также посредством общения в социальных сетях: полный номер карточки, срок ее действия, код CVC/CVV (находящиеся на обратной стороне карты), логин и пароль к интернет-банкингу, паспортные данные, кодовое слово (цифровой код) из SMS-сообщений.

В случае если «сотрудник банка» в разговоре сообщает, что с карточкой происходят несанкционированные транзакции, необходимо отвечать, что вы придете в банк лично, – все подобные вопросы нужно решать в отделении банка, а не по телефону.

**ВНИМАНИЕ:** *помните, что сотрудники банковских учреждений никогда не используют для связи с клиентом мессенджеры (Viber, Telegram, WhatsApp)*.

2. Для осуществления онлайн-платежей необходимо использовать только надежные платежные сервисы, **обязательно проверяя доменное имя ресурса в адресной строке браузера**.

3. **Не следует хранить банковские карты, их фотографии и реквизиты в местах, которые могут быть доступны посторонним лицам**; это же относится к фотографиям и иным видам информации конфиденциального характера.

4. Следует **воздерживаться от осуществления онлайн-платежей, связанных с предоплатой и перечислением задатков за товары и услуги**, благотворительной и спонсорской помощи в пользу организаций и физических лиц при отсутствии достоверных данных о том, что названные субъекты являются теми, за кого себя выдают.

5. Не стоит перечислять денежные средства на счета электронных кошельков, карт-счета банковских платежных карточек, счета SIM-карт **по просьбе пользователей сети Интернет**.

– использовать отдельную карту для Интернет-покупок и не хранить на ней деньги;

– подключить услуги 3D-Secure, SMS-информирование, установить необходимые лимиты;

6. Для доступа к системам дистанционного банковского обслуживания (интернет-банкинг, мобильный банкинг), электронным почтовым ящикам, аккаунтам социальных сетей и иным ресурсам **необходимо использовать сложные пароли, исключающие возможность их подбора**. Стоит воздержаться от паролей: дат рождения, имен, фамилий – то есть тех, которые легко вычислить из общедоступных источников информации (например, тех же социальных сетей).

7. При составлении платежных документов **важно проверять платежные реквизиты получателя денежных средств**.

8. При поступлении в социальных сетях сообщений от лиц, состоящих в категории «друзья», с просьбами о предоставлении реквизитов банковских платежных карточек **не следует отвечать на подобные сообщения, а необходимо связаться с данными пользователями напрямую посредством иных средств связи**.

9. При обнаружении факта взлома аккаунтов социальных сетей необходимо незамедлительно восстанавливать к ним доступ с помощью службы поддержки либо блокировать, а также предупреждать об этом факте лиц, с которыми общались посредством данных социальных сетей.

10. **Нельзя открывать файлы, поступающие с незнакомых адресов электронной почты и аккаунтов мессенджеров**; не переходить по ссылкам в сообщениях о призах и выигрышах.

11. Необходимо **использовать лицензионное программное обеспечение, регулярно обновлять программное обеспечение и операционную систему; установить антивирусную программу** не только на персональный компьютер, но и на смартфон, планшет и регулярно обновлять ее.

12. Следует **ознакомить с перечисленными правилами безопасности своих родственников и знакомых**, которые в силу возраста или недостаточного уровня финансовой грамотности могут быть особенно уязвимы для действий киберпреступников.

В любой ситуации необходимо проявлять бдительность и своими действиями не создавать условия для совершения в отношении Вас преступлений.

В случае совершения в отношении Вас противоправных деяний либо обнаружения факта совершения преступления, рекомендуем Вам в кратчайшие сроки обратиться в органы внутренних дел по месту жительства.

**ОТВЕТСТВЕННОСТЬ ПО КИБЕРПРЕСТУПЛЕНИЯМ**

В уголовном праве Беларуси закреплена ответственность за ряд преступлений против информационной безопасности (Глава 31 УК РБ):

Статья 349. Несанкционированный доступ к компьютерной информации. Наказание: штраф, арест, ограничение или лишение свободы на срок до 2 лет. Если действия, предусмотренные статьей, повлекли тяжкие последствия – возможно ограничение свободы на срок до 5 лет или лишением свободы на срок до 7 лет.

Статья 350. Модификация компьютерной информации. Наказание: штраф, лишение права занимать определенные должности или заниматься определенной деятельностью, арест, ограничение свободы на срок до 5 лет, лишение свободы на срок до 7 лет.

Статья 351. Компьютерный саботаж – умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя. Наказание: штраф, лишение права занимать определенные должности или заниматься определенной деятельностью, арест, ограничение свободы на срок до 5 лет, лишение свободы на срок 3-10 лет.

Статья 352. Неправомерное завладение компьютерной информацией наказывается общественными работами, или штрафом, или арестом на срок до шести месяцев, или ограничением или лишением свободы на срок до 2 лет.

Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети наказывается штрафом, или арестом на срок 3-6 месяцев, или ограничением свободы на срок до 2 лет.

Статья 354. Разработка, использование либо распространение вредоносных программ. Наказание: штраф, арест, ограничение свободы на срок до 2 лет, лишение свободы до 10 лет.

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети. Наказание: штраф, лишение права занимать определенные должности или заниматься определенной деятельностью, исправительные работы на срок до 2 лет, ограничение свободы на срок до 5 лет, лишение свободы на срок до 7 лет.

В целом этот перечень преступлений соответствует положениям Конвенции Совета Европы о компьютерных преступлениях (2001 г.), к которой Беларусь не присоединилась. В Конвенции такие преступления перечислены в группе **правонарушений против конфиденциальности, целостности и доступности компьютерных данных и систем**. Помимо этой группы Конвенция выделяет также **преступления, связанные с использованием компьютерных средств**: подлог и мошенничество, совершенные с использованием компьютерных технологий.

В **Уголовном Кодексе Республики Беларусь** к подобным преступлениям относят

хищение путем использования компьютерной техники (Ст. 212);

причинение имущественного ущерба без признаков хищения (Ст. 216, путем модификации компьютерной информации);

ряд составов, которые включают хищение (Ст. 294, 323, 327, 333).

Третья группа преступлений включает преступления, связанные с содержанием компьютерных данных: детская порнография, нарушение авторского права.

В Беларуси установлены широкие запреты в отношении всех порнографических материалов. При этом учтены положения Конвенции: в ст. 343 и ст. 343-1 УК РБ распространение порнографических материалов посредством сети Интернет является квалифицирующим признаком (Статья 343 УК РБ. Изготовление и распространение порнографических материалов или предметов порнографического характера).

В отношении нарушений авторских прав с использованием компьютерных технологий уголовное право Республики Беларусь не предусматривает каких-либо специальных норм.

Некоторые из рассмотренных составов преступлений имеют свои аналоги в Кодексе об административных правонарушениях (Статья 23.4 КоАП РБ. Hесанкционированный доступ к компьютерной информации; cтатья 11.2 КоАП РБ. Причинение имущественного ущерба). Основное отличие – размер ущерба и степень общественной опасности деяний.

Примечательно также наличие в **Кодексе об административных правонарушениях ответственности** за пропаганду и (или) публичное демонстрирование, изготовление и (или) распространение нацистской символики или атрибутики (Ст. 19.10.), в том числе с использованием сети интернет. Подобная ответственность согласуется с положениями ст. 3 Дополнительного протокола к Конвенции 2001 г., относящемуся к ответственности за акты расистской и ксенофобской природы, совершенные посредством компьютерных систем.

