ПРОФИЛАКТИКА И ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ

Киберпреступления – 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.)

Основные понятия, которые относятся к теме безопасного поведения в сети интернет и описывают виды киберпреступлений

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.). Источник (<https://www.oac.gov.by/fighting-telecom-fraud/phishing>)

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. Источник (<https://www.oac.gov.by/phishing/fighting-telecom-fraud/vishing>)

Информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере. Источник (https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf)

Кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организаций взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации. Источник (https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf)

Кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз. Источник (https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf)

Киберинцидент – событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политик безопасности. Источник (https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf)

Кибертерроризм – атаки на информационные системы, несущие угрозу здоровью и жизни людей, а также способные спровоцировать серьезные нарушения функционирования критически важных объектов в целях оказания воздействия на принятие решений органами власти, либо воспрепятствования политической или иной общественной деятельности, либо устрашения населения, либо дестабилизации общественного порядка. Источник

(https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf)

Конфиденциальность информации – требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь. Источник

(<https://pravo.by/document/?guid=3871&p0=H10800455>)

Обладатель информации – субъект информационных отношений, получивший права обладателя информации по основаниям, установленным актами законодательства Республики Беларусь, или по договору. Источник

(<https://pravo.by/document/?guid=3871&p0=H10800455>)

Персональные данные – основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами Республики Беларусь внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо. Источник

(<https://pravo.by/document/?guid=3871&p0=H10800455>)

Пользователь информации – субъект информационных отношений, получающий, распространяющий и (или) предоставляющий информацию, реализующий право на пользование ею. Источник

(<https://pravo.by/document/?guid=3871&p0=H10800455>)

Пользователь информационной системы и (или) информационной сети – субъект информационных отношений, получивший доступ к информационной системе и (или) информационной сети и пользующийся ими. Источник

(<https://pravo.by/document/?guid=3871&p0=H10800455>)

Предоставление информации – действия, направленные на ознакомление с информацией определенного круга лиц. Источник

(<https://pravo.by/document/?guid=3871&p0=H10800455>)

Преступления в информационной сфере – предусмотренные Уголовным кодексом Республики Беларусь преступления против информационной безопасности (киберпреступления) и иные преступления, предметом или средством совершения которых являются информация, информационные системы и сети. Источник

(https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf)

Распространение информации – действия, направленные на ознакомление с информацией неопределенного круга лиц. Источник (<https://pravo.by/document/?guid=3871&p0=H10800455>)

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. Источник (<https://pravo.by/document/?guid=3871&p0=H10800455>)

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. Источник (<https://www.oac.gov.by/phishing/fighting-telecom-fraud/smishing>)

ПРОФИЛАКТИЧЕСКИЙ МАТЕРИАЛ (<https://disk.yandex.by/d/F03-laudj7830g>)

Материалы по вопросам кибербезопасности и Рекомендации о том, как не стать жертвой кибермошенников

Материалы с сайта МВД Республики Беларусь (<https://www.mvd.gov.by/ru/news/7021>)

Киберпреступность в Беларуси (<https://belta.by/infographica/view/kiberprestupnost-v-belarusi-24963/>)

Как не стать жертвой вишинга (<https://belta.by/infographica/view/kak-ne-stat-zhertvoj-vishinga-24468/>)

Как не стать жертвой фишинга (<https://belta.by/infographica/view/kak-ne-stat-zhertvoj-fishinga-24467/>)

Как не стать жертвой интернет-мошенников (<https://belta.by/infographica/view/kak-ne-stat-zhertvoj-internet-moshennikov-24466/>)

Как не стать жертвой киберпреступника. Защита банковской карточки (<https://belta.by/infographica/view/kak-ne-stat-zhertvoj-kiberprestupnika-zaschita-bankovskoj-kartochki-16627/>)

Рекомендации о том, как не стать жертвой кибермошенников и информация об уголовной ответственности за киберпреступления (<https://belta.by/infographica/view/kak-ne-stat-zhertvoj-kiberprestupnika-zaschita-bankovskoj-kartochki-16627/>)

В Уголовном кодексе Республики Беларусь содержится ряд статей, предусматривающих уголовную ответственность за киберпреступления:

ст.212 «Хищение путем использования компьютерной техники»;

ст.349 «Несанкционированный доступ к компьютерной информации»;

ст.350 «Модификация компьютерной информации»;

ст.351 «Компьютерный саботаж»;

ст.352 «Неправомерное завладение компьютерной информацией»;

ст.353 «Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети»;

ст.354 «Разработка, использование либо распространение вредоносных программ»;

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

Если Вы стали жертвой киберпреступников, обращайтесь в главное управление по противодействию киберпреступности криминальной милиции МВД Беларуси (<https://www.mvd.gov.by/ru/page/upravlenie-k>)

Telegram канал «Цифровая грамотность». Канал о том, как не стать жертвой мошенников в интернете (<https://t.me/s/cifgram>)