

# Кибербезопасность

**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.).

**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.

**Информационная безопасность** – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

**Кибератака** – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

**Кибербезопасность** – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз.

**Кибербуллинг** – это травля с использованием цифровых технологий. Кибербуллинг может происходить в социальных сетях, мессенджерах, на игровых платформах и в мобильных телефонах. Это целенаправленная

модель поведения, которая ставит своей задачей запугать, разозлить или опозорить того, кто стал объектом травли.

- Что такое кибербуллинг и как от него защититься
- Основано на реальных событиях: история кибербуллинга
- Кибербуллинг. Меня обижают в Интернете
- Кибербуллинг. Я — свидетель травли в Интернете

**Киберинцидент** – событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политик безопасности.

[https://www.youtube.com/watch?v=bGmnK\\_ruQ-M](https://www.youtube.com/watch?v=bGmnK_ruQ-M)

[https://www.youtube.com/watch?v=-eEFJ\\_jz5IM](https://www.youtube.com/watch?v=-eEFJ_jz5IM)

<https://www.youtube.com/watch?v=frWLJG9KIAQ>

<https://www.youtube.com/watch?v=Di37YwjBVog>

**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.

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

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

**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.

**Нежелательный контент** – это не только материалы (картинки, видео, аудио, тексты), содержащие насилие, порнографию, пропаганду наркотических средств, азартных игр, но и различные вредоносные и шпионские программы, задача которых получить доступ к информации на компьютере владельца. Также к нежелательному контенту относятся сайты, запрещенные законодательством.

**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.

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

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

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

**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

**Распространение информации** – действия, направленные на ознакомление с информацией неопределенного круга лиц. Источник

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

**Скам** (scam – с англ. яз. афера, мошенничество) – это мошенничество в сети Интернет. Источник

**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

**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

**Цифровая гигиена** – это свод правил, следуя которым, человек обеспечивает себе информационную безопасность (не анонимность, а защиту) в сети Интернет. Относится к сфере знаний о цифровой безопасности. Источник

**Smishing** (использование текстовых сообщений SMS) – это метод, похожий на фишинг, но вместо отправки электронных писем злоумышленники отправляют текстовые сообщения своим потенциальным жертвам. Вы получаете срочное текстовое сообщение на свой смартфон с прикрепленной ссылкой, в которой говорится, что оно принадлежит вашему банку и вам необходимо получить к нему доступ, чтобы обновить банковскую информацию или другую информацию онлайн-банкинга.

## ОТВЕТСТВЕННОСТЬ

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»

- Сайт МВД Республики Беларусь

<https://www.mvd.gov.by/ru/media/photo/326>

- 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>

- Цифровая гигиена (для детей)

[https://moiro.by/files/00206/obj/140/185383/doc/Памятка\\_Цифровая%20гигиена\\_Дети.pdf](https://moiro.by/files/00206/obj/140/185383/doc/Памятка_Цифровая%20гигиена_Дети.pdf)

- Цифровая гигиена (для родителей)

[https://moiro.by/files/00206/obj/140/185383/doc/Памятка\\_Цифровая%20гигиена\\_Родители.pdf](https://moiro.by/files/00206/obj/140/185383/doc/Памятка_Цифровая%20гигиена_Родители.pdf)

- Компьютерная безопасность

[https://moiro.by/files/00206/obj/140/185383/doc/Памятка\\_Компьютерная%20безопасность.pdf](https://moiro.by/files/00206/obj/140/185383/doc/Памятка_Компьютерная%20безопасность.pdf)

- Цифровая гигиена (для детей)

[https://moiro.by/files/00206/obj/140/185393/doc/Буклет\\_цифровая%20гигиена\\_Дети.pdf](https://moiro.by/files/00206/obj/140/185393/doc/Буклет_цифровая%20гигиена_Дети.pdf)

- Цифровая гигиена (для родителей)

[https://moiro.by/files/00206/obj/140/185393/doc/Буклет\\_цифровая%20гигиена\\_Родители.pdf](https://moiro.by/files/00206/obj/140/185393/doc/Буклет_цифровая%20гигиена_Родители.pdf)

- Борьба с киберпреступностью

<https://expert.belta.by/page21683498.html>

- [Киберликбез](#)

<https://mvd.gov.by/ru/news/8099>