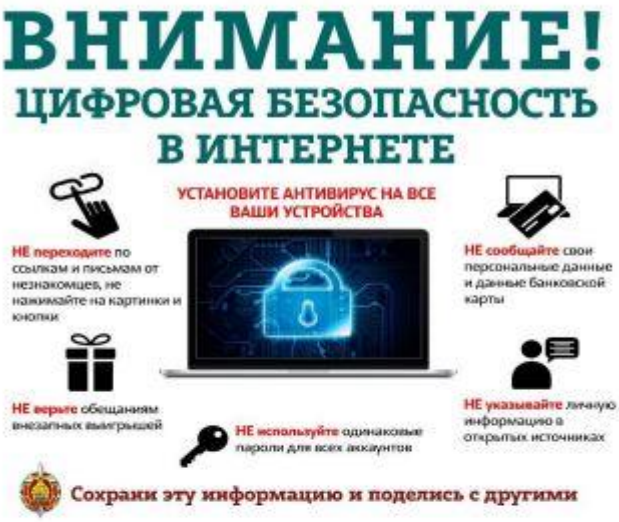
КИБЕРБЕЗОПАСНОСТЬ

Проблема безопасного поведения в интернете – актуальная проблема сегодняшнего дня как для несовершеннолетних детей, так и для взрослого человека. Как не стать жертвой киберпреступника? Как сохранить в безопасности свою личную информацию, размещенную в интернете? Как не допустить совершения противоправных поступков в Сети Интернет?

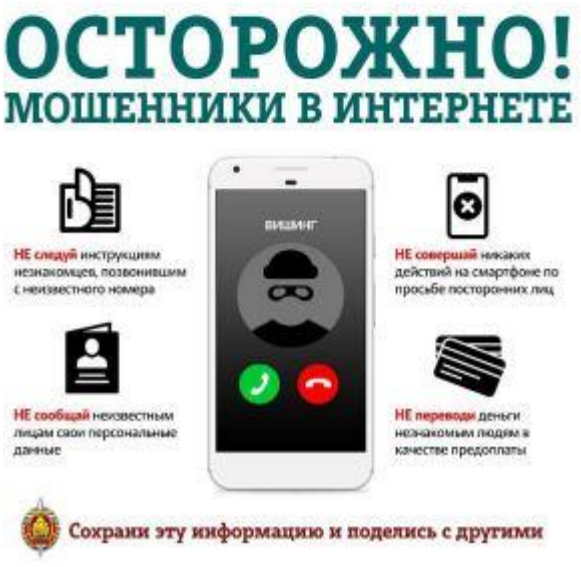
Киберпреступление — вид правонарушения, непосредственно связанного с использованием компьютерных технологий и сети Интернет, включающий в себя распространение вирусов, нелегальную загрузку файлов, кражу персональной информации, например информации по банковским счетам. *Киберпреступлениями считаются те преступления, в которых ведущую роль играют компьютер или компьютерная сеть.*



Важной особенностью преступлений против компьютерной информации и преступлений, совершенных путем использования компьютерной техники, является их транснациональный характер, поскольку они подпадают под все критерии, предусмотренные Конвенцией Организации Объединенных Наций против транснациональной организованной преступности (заключена в г. Палермо 15.11.2000), участницей которой является и Республика Беларусь

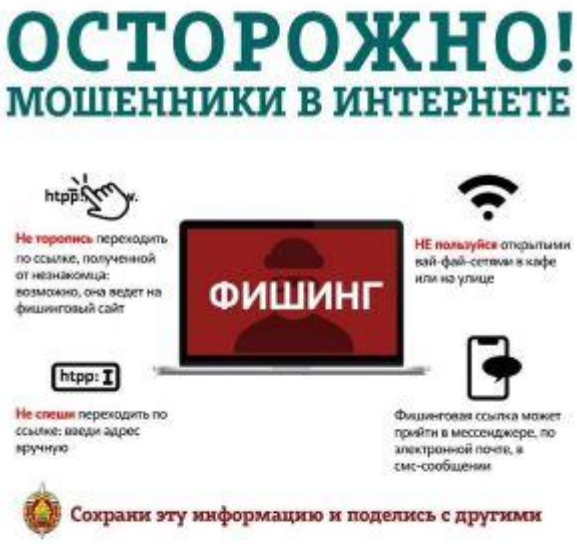
Многочисленные факты выявления и установления закономерностей механизмов развития новых видов преступлений, связанных с использованием средств компьютерной техники и информационных технологий, показывают, что сама компьютерная техника может быть как предметом преступного посягательства, так и инструментом совершения преступления.

По способу совершения, наибольшая часть киберпреступлений, с использованием сети Интернет, совершалась путем *«вишинга»* и применения *«фишинговых»* инструментов.



Вишинг *(англ. vishing, от Voice phishing) - один из методов мошенничества с использованием социальной инженерии, который заключается в том, что 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 карт - счетом/платежной картой.*

Фишинг *(англ. phishing от fishing «рыбная ловля, выуживание») - вид интернет - мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам и паролям.*



Основной причиной роста преступлений по линии противодействия киберпреступности, является:

1.Постоянное увеличение количества банковских платежных карт, находящихся у держателей, так и совершаемым по ним операциям, в том числе в сети Интернет, системах «Интернет и мобильный банкинг»;

2.Беспечность, либо излишняя доверчивость граждан, позволяющая злоумышленнику завладеть реквизитами доступа к учетным записям посредством использования методов социальной инженерии, фишинговых сообщений, поддельных интернет - ресурсов, использования троянских и иных вредоносных программ;

3.Преднамеренные действия и ошибки персонала информационных систем, выражающиеся в нарушении установленных регламентов их эксплуатации и правил обработки информации;

4.Использование простых паролей (зачастую совпадающих с именем пользователя, либо использования номера своих мобильных телефонов, «qwerty», «qwerty1234», и т.д.) для доступа к учетным записям различных развлекательных и финансовых сетевых ресурсов;

5.Присутствие (появление) различных уязвимостей в информационных системах и наличие просчетов в системе безопасности банковских и финансовых учреждений;

6.Доступность и относительная простота использования различных инструментов (специализированных программных обеспечений и сервисов), в том числе средств анонимизации (VPN, прокси - сервера, VDS, VPS, TOR-браузер и т.д.) использующие функцию подмены IP - адресов, распространяемых в сети Интернет.

7.Простота механизма получения «логина» и «пароля» пользователей к их персональным страница, а именно наличие большого количества инструкций, с примерами специальных кодов и специализированных сервисов, направленных на «фишинговое» (получения различными способами сведений у пользователей о реквизитах доступа к их учетным записям, аккаунтам, электронным почтовым ящикам и т.д.) завладение указанными данными.

Чтобы обезопасить себя при встрече с таким методом киберпреступлений, необходимо хотя бы соблюдать минимальные требования безопасности

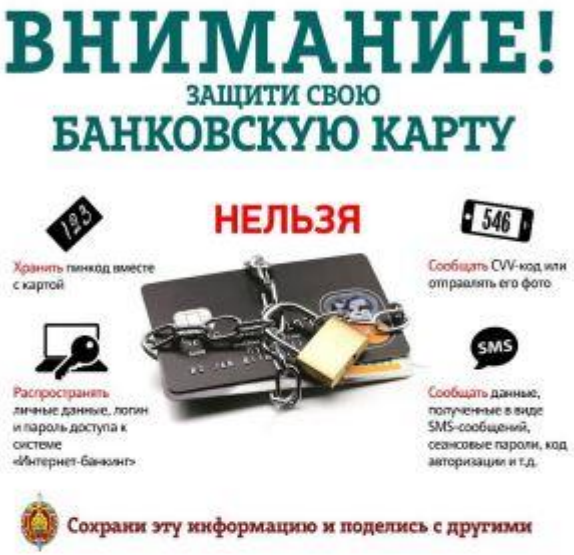
Рекомендации по соблюдению мер информационной безопасности

1. Защита данных банковской платежной карточки

Необходимо:

- Хранить в тайне пин-код, сведения с карточки сеансовых кодов;
- Прикрывать ладонью клавиатуру при вводе пин-кода;
- Оформить отдельную карту для онлайн-покупок, выезда за границу и не хранить на ней большие суммы. Для карты, используемой в РБ рекомендуется ограничить возможность ее использования за пределами РБ;

- Использовать двухфакторную аутентификацию, услугу «3-D Sequre», установить лимиты на максимальные суммы операций, подключить смс-оповещение о проведении операций по карте;
- Скрыть CVV (CVC) номер на карте (трехзначный номер на оборотной стороне), предварительно сохранив его;
- Вводить «логин» и «пароль» к системе «Интернет-банкинг» только на официальном сайте или в мобильном приложении банка;
- В случае утери (кражи) карты, незамедлительно по телефону обратиться в банк для ее блокирования;
- При обнаружении несанкционированного списания денежных средств с карт-счета, незамедлительно обратиться с заявлением в банк для их возврата по принципу «нулевой ответственности».



Не рекомендуется:

- Хранить пин-код вместе с карточкой/на карточке;
- Сообщать кому-либо реквизиты карты или отправлять их фото по сети Интернет;
- Распространять свои персональные данные (информацию личного характера, номер мобильного телефона), «логин» и «пароль» доступа к системе «Интернет-банкинг»;
- Сообщать данные, полученные в виде SMS-сообщений: сеансовые пароли, код авторизации, пароль «3-D Sequre» и т.д.;
- Пользоваться системой «Интернет-банкинг» на чужих компьютерах или мобильных устройствах.

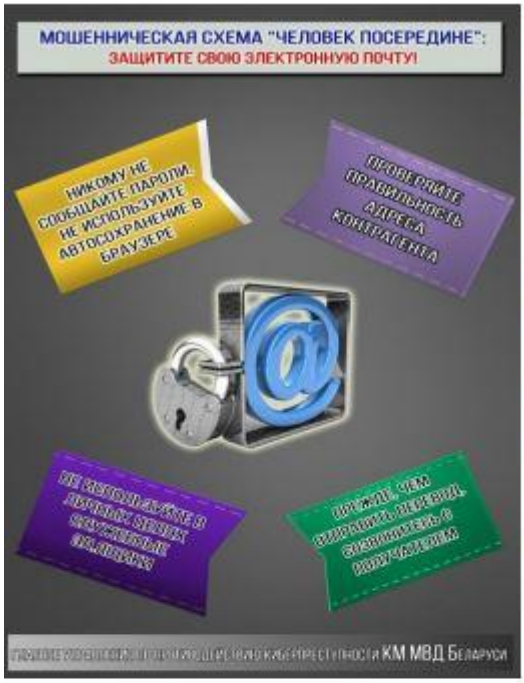
2. Безопасность электронной почты

Необходимо:

- Подключить двухфакторную аутентификацию;
- Использовать минимум 2 типа e-mail адресов: закрытые (только для привязки устройств и средств защиты, интернет-банкинга и др.), открытые (отдельные для переписки, регистрации на форумах, оформления различных подписок и т.д.);
- Использовать спам-фильтры;
- В случае подозрительных ситуаций проверить статистику подключений и изменить пароль.

Не рекомендуется:

- Реагировать на письма от неизвестного отправителя: скорее всего это спам или мошенники;



- Открывать подозрительное вложение к письму: сначала позвоните отправителю и узнайте, что это за файл;
- Отправлять в открытом виде важные данные (фотоизображения документов, пароли и т.д.). В случае необходимости – заархивировать, установив сложный пароль.

3. Надежные пароли

Необходимо:

- Создавать персональные (уникальные) пароли к разным сервисам;
- Использовать сложные пароли: минимум 10 символов, одновременно цифры, строчные и прописные символы, знаки пунктуации и другие символы;
- Доверять только проверенным менеджерам паролей;
- Регулярно производить смену паролей.

Не рекомендуется:

- Хранить пароли на бумажных носителях, рабочем столе компьютера и в других легкодоступных местах, а также передавать их кому-либо;
- Использовать повторения символов;
- Использовать в качестве пароля свой логин (имя пользователя, учетной записи, никнейм, дату рождения и т.д.);
- Сохранять пароль автоматически в браузере;
- Использовать биографическую информацию и сведения, размещенные в социальной сети.

4. Проверенные браузеры и сайты

Необходимо:

- Использовать специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать посещения сомнительных сайтов;
- Производить регулярное обновление ПО, антивирусов;
- Обращать внимание при авторизации на доменное имя интернет-ресурса (может произойти подмена имени сайта).

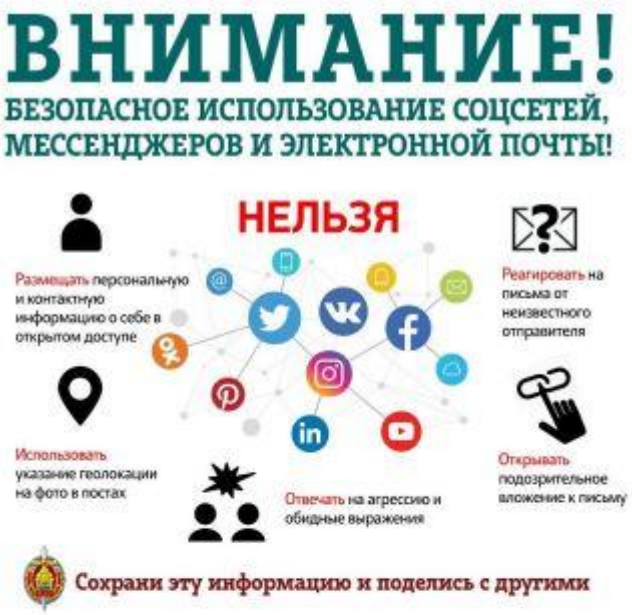
Не рекомендуется:

- Переходить по непроверенным ссылкам и посещать сайты сомнительного содержания;
- Вводить информацию на сайтах, если соединение не защищено (нет https);
- Открывать всплывающие окна, рекламные баннеры и устанавливать предлагаемое неизвестными сайтами ПО.

5. Использование приложений, соцсетей и мессенджеров

Неоходимо:

- По возможности скрывать номер телефона, адрес электронной почты и другие сведения;
- Обмениваться сообщениями в соцсетях и мессенджерах только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения.



Не рекомендуется:

- Размещать персональную и контактную информацию о себе в открытом доступе;
- Использовать указание геолокации на фото и постах;
- Отвечать на обидные выражения и агрессию в соцсетях – лучше написать об этом администратору ресурса;
- Употреблять ненормативную лексику при общении;
- Размещать в Интернет объявления с указанием используемых номеров телефонов, а также указывать контактные данные мессенджеров. В случае размещения – удалять сразу же по миновании надобности.

6. Безопасность мобильных устройств

Необходимо:

- Использовать пин-код, а также дополнительные способы блокирования устройства (графический ключ, пароль, отпечаток пальца и др.);
- Своевременно обновлять операционную систему устройства, антивирус и др. ПО;
- Устанавливать приложения из PlayMarket, AppStore или только из проверенных источников;
- Обращать внимание, к каким функциям гаджета приложение запрашивает доступ;
- Включить встроенные функции устройства для определения его местонахождения;
- В случае утери (кражи) устройства, незамедлительно сменить пароли к интернет-банкингу, электронной почте и другим сервисам, а также обратиться в правоохранительные органы;
- При смене абонентского номера обязательно изменить привязку интернет-сервисов к новому номеру (лучше сделать это заблаговременно);
- При продаже устройства произвести его сброс до заводских настроек.

Не рекомендуется:

- Передавать незнакомым мобильный телефон или сим-карту. В случае передачи – контролировать все действия, которые производятся с устройством;
- Устанавливать приложения с низким рейтингом и отрицательными отзывами;
- Перезванивать на незнакомые иностранные номера;
- Хранить важную информацию на мобильном устройстве;
- Делать полное снятие ограничения на устройстве ("джейлбрейк").

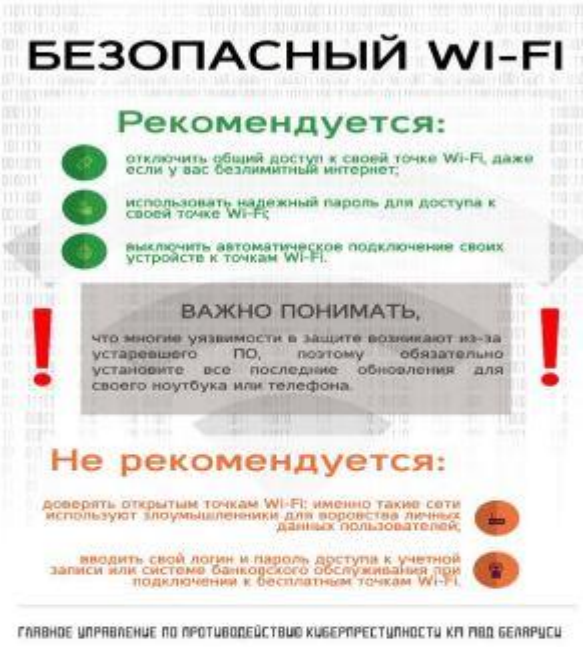
7. Безопасный Wi-Fi

Необходимо:

- Отключить общий доступ к своей Wi-Fi точке, даже если у вас «безлимитный» Интернет;
- Использовать надежный пароль для доступа к вашей Wi-Fi точке;
- Деактивировать автоматическое подключение своих устройств к открытым Wi-Fi точкам.

Не рекомендуется:

- Вводить свой логин и пароль доступа к учетной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговом центре и т.д.



Рекомендации для родителей по профилактике киберпреступлений среди несовершеннолетних.

1. Установите с ребенком доверительные отношения и положительный эмоциональный контакт в вопросе использования сети Интернет. Оговорите с ребенком критический уровень опасности, когда решение в возникшей проблемной ситуации должно приниматься родителями (иным доверенным лицом, обладающим достаточным опытом и познаниями, например, старшим братом или сестрой) либо по согласованию с ними.
2. Установленные для ребенка правила работы в сети Интернет должны соответствовать его возрасту и развитию. Применение слишком мягких правил на начальном этапе освоения сети ребенком может повысить риск возникновения у ребенка различных угроз. А слишком жесткие правила либо запреты для ребенка могут повлечь игнорирование им всяких правил.
3. Ребенку для работы в сети Интернет должен быть предоставлен в пользование компьютер со специфически настроенными параметрами. В обязательном порядке на компьютере должно быть установлено и настроено актуальное антивирусное программное обеспечение, установлен и настроен сетевой экран. Родителями должен контролироваться перечень установленного на компьютере программного обеспечения и его настройки.

4. Интересуйтесь, какими сайтами и программами пользуются Ваши дети; настаивайте на том, чтобы подросток не соглашался на встречу с друзьями из Интернета; напоминайте о необходимости обеспечения конфиденциальности личной информации; предостерегайте детей от использования сети для хулиганства либо совершения иных противоправных деяний, разъясните суть и ответственность за совершение преступлений против информационной безопасности.
5. В случае установления фактов совершения противоправных деяний в сети Интернет в отношении детей рекомендуем родителям не умалчивать данные факты, а сообщать о них в зависимости от ситуации куратору учебной группы, педагогу социальному учреждения образования, в правоохранительные органы по месту жительства.

Ответственность за совершение киберпреступлений

Напоминаем, что несовершеннолетние несут уголовную ответственность за совершение киберпреступлений с 16 лет, за совершение преступления, предусмотренного ст.212 УК РБ – с 14 лет!

Статья 212. Хищение имущества путем модификации компьютерной информации
(в ред. Закона Республики Беларусь от 26.05.2021 N 112-З)

1. Хищение имущества путем модификации компьютерной информации -

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. То же деяние, совершенное повторно либо группой лиц по предварительному сговору, -

наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, совершенные в крупном размере, -

наказываются ограничением свободы на срок от двух до пяти лет или лишением свободы на срок от двух до семи лет со штрафом или без штрафа и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

4. Деяния, предусмотренные частями 1, 2 или 3 настоящей статьи, совершенные организованной группой либо в особо крупном размере, -

наказываются лишением свободы на срок от пяти до двенадцати лет со штрафом и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Статья 349. Несанкционированный доступ к компьютерной информации
(в ред. Закона Республики Беларусь от 26.05.2021 N 112-З)

1. Несанкционированный доступ к компьютерной информации, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), совершенный из корыстной заинтересованности либо повлекший по неосторожности причинение существенного вреда, -

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

2. Несанкционированный доступ к компьютерной информации либо самовольное пользование компьютерной системой или сетью, повлекшие по неосторожности крушение,

4. Интересуйтесь, какими сайтами и программами пользуются Ваши дети; настаивайте на том, чтобы подросток не соглашался на встречу с друзьями из Интернета; напоминайте о необходимости обеспечения конфиденциальности личной информации; предостерегайте детей от использования сети для хулиганства либо совершения иных противоправных деяний, разъясните суть и ответственность за совершение преступлений против информационной безопасности.
5. В случае установления фактов совершения противоправных деяний в сети Интернет в отношении детей рекомендуем родителям не умалчивать данные факты, а сообщать о них в зависимости от ситуации куратору учебной группы, педагогу социальному учреждения образования, в правоохранительные органы по месту жительства.

Ответственность за совершение киберпреступлений

Напоминаем, что несовершеннолетние несут уголовную ответственность за совершение киберпреступлений с 16 лет, за совершение преступления, предусмотренного ст.212 УК РБ – с 14 лет!

Статья 212. Хищение имущества путем модификации компьютерной информации
(в ред. Закона Республики Беларусь от 26.05.2021 N 112-З)

1. Хищение имущества путем модификации компьютерной информации -

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. То же деяние, совершенное повторно либо группой лиц по предварительному сговору, -

наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, совершенные в крупном размере, -

наказываются ограничением свободы на срок от двух до пяти лет или лишением свободы на срок от двух до семи лет со штрафом или без штрафа и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

4. Деяния, предусмотренные частями 1, 2 или 3 настоящей статьи, совершенные организованной группой либо в особо крупном размере, -

наказываются лишением свободы на срок от пяти до двенадцати лет со штрафом и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Статья 349. Несанкционированный доступ к компьютерной информации
(в ред. Закона Республики Беларусь от 26.05.2021 N 112-З)

1. Несанкционированный доступ к компьютерной информации, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), совершенный из корыстной заинтересованности либо повлекший по неосторожности причинение существенного вреда, -

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

2. Несанкционированный доступ к компьютерной информации либо самовольное пользование компьютерной системой или сетью, повлекшие по неосторожности крушение,

аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, -

наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет.

Статья 350. Уничтожение, блокирование или модификация компьютерной информации

(в ред. Закона Республики Беларусь от 26.05.2021 N 112-З)

1. Умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации, разрушение, блокирование либо нарушение работы компьютерной системы, сети или машинного носителя либо модификация компьютерной информации при отсутствии признаков преступления против собственности, повлекшие причинение существенного вреда, -

наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. Те же деяния, совершенные повторно либо группой лиц по предварительному сговору, -

наказываются штрафом, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, повлекшие по неосторожности последствия, указанные в части 2 статьи 349 настоящего Кодекса, -

наказываются лишением свободы на срок от трех до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Статья 352. Неправомерное завладение компьютерной информацией

(в ред. Закона Республики Беларусь от 26.05.2021 N 112-З)

1. Умышленные несанкционированное копирование, перехват компьютерной информации либо иное неправомерное завладение компьютерной информацией, повлекшие причинение существенного вреда, -

наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на срок до двух лет.

2. Те же деяния, совершенные повторно либо группой лиц по предварительному сговору, -

наказываются штрафом, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, повлекшие по неосторожности последствия, указанные в части 2 статьи 349 настоящего Кодекса, -

наказываются лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Статья 354. Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств

(в ред. Закона Республики Беларусь от 26.05.2021 N 112-З)

1. Разработка, использование, распространение либо сбыт компьютерной программы или специального программного или аппаратного средства, заведомо предназначенных для нарушения системы защиты, несанкционированного доступа к компьютерной системе, сети

или машинному носителю, несанкционированного уничтожения, блокирования, модификации компьютерной информации или неправомерного завладения компьютерной информацией либо нарушения работы компьютерной системы, сети или машинного носителя, -

наказываются штрафом, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. Те же действия, совершенные группой лиц по предварительному сговору, -

наказываются штрафом, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Действия, предусмотренные частями 1 или 2 настоящей статьи, повлекшие по неосторожности последствия, указанные в части 2 статьи 349 настоящего Кодекса, -

наказываются лишением свободы на срок от трех до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети

(в ред. Закона Республики Беларусь от 26.05.2021 N 112-З)

1. Умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этим системе или сети, повлекшее по неосторожности причинение существенного вреда, -

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок до двух лет, или ограничением свободы на тот же срок.

2. То же деяние, повлекшее по неосторожности последствия, указанные в части 2 статьи 349 настоящего Кодекса, -

наказывается ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Материал подготовлен педагогом социальным филиала БНТУ БГПК с использованием данных, предоставленных отделением по противодействию киберпреступности криминальной милиции Борисовского РУВД

24.11.2021