Памятка об ответственности за совершение киберпреступлений и методы противодействия киберпреступности

Уголовная ответственность за совершение киберпреступлений (преступлений в сфере компьютерной информации - Глава 28 Уголовного кодекса Российской Федерации)

Статья 272. Неправомерный доступ к компьютерной информации

(в ред. Федерального закона от 07.12.2011 N 420-ФЗ)

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, -

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

(в ред. Федерального закона от 28.06.2014 N 195-ФЗ)

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, -

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы

на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до семи лет.

Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

(в ред. Федерального закона от 07.12.2011 N 420-ФЗ)

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет

со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до семи лет.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

(в ред. Федерального закона от 07.12.2011 N 420-ФЗ)

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, -

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Защита от киберпреступлений

Учитывая распространенность киберпреступлений, есть ли способ их предотвратить? Вот несколько советов по защите вашего компьютера и персональных данных от киберпреступников.

1. Регулярное обновление ПО и операционной системы

Регулярное обновление программного обеспечения и операционной системы гарантирует наличие на компьютере актуальных исправлений безопасности.

2. Использование антивирусных программ и их регулярное обновление

Использование антивирусного или комплексного защитного решения для интернет-безопасности, например Kaspersky Premium, – хороший способ защитить вашу систему от кибератак. Антивирусные программы позволяют сканировать систему, обнаруживать и нейтрализовать угрозы до того, как они смогут навредить. Качественная антивирусная защита не допустит киберпреступников до компьютера и поможет сохранить ваши данные, пока вы спокойно занимаетесь своими делами. Для полной безопасности регулярно обновляйте антивирусное ПО.

3. Использование надежных паролей

Устанавливайте надежные пароли, которые никто не сможет подобрать, и не храните их в записанном виде. Также можно использовать проверенный менеджер паролей, который случайным образом сгенерирует надежные пароли за вас.

4. Привычка не открывать вложенные файлы в письмах

При помощи вложений в спам-письмах киберпреступники реализуют разные виды атак, включая заражение компьютера вредоносными программами. Никогда не открывайте вложенные файлы от неизвестных отправителей.

5. Привычка не переходить по ссылкам в спам-письмах и на недоверенных веб-сайтах

Люди нередко становятся жертвами киберпреступников, переходя по ссылкам в спам-письмах и других сообщениях, а также на незнакомых веб-сайтах. Чтобы оставаться в безопасности, никогда не переходите по таким ссылкам.

6. Осторожность при передаче личной информации

Никогда не сообщайте свои персональные данные по телефону или электронной почте, если не до конца уверены в безопасности ваших коммуникаций. Убедитесь, что ваш собеседник действительно тот, за кого себя выдает.

7. Общение по официальным каналам

Если вам позвонили из организации и в ходе разговора запросили ваши персональные данные, повесьте трубку. Перезвоните по номеру, указанному на официальном веб-сайте компании, чтобы убедиться, что вы разговариваете не с киберпреступником, а с реальным сотрудником. Лучше

всего позвонить с другого телефона, так как киберпреступники могут держать прежнюю линию связи открытой. В этом случае вы будете думать, что перезвонили по официальному номеру, тогда как на самом деле продолжите разговаривать со злоумышленниками, которые притворяются представителями банка или другой организации.

8. Внимательность при посещении веб-сайтов

Обращайте внимание на URL-адреса ссылок, по которым переходите. Убедитесь, что адрес подлинный. Не переходите по ссылкам, URL-адреса которых вам незнакомы или выглядят как спам. Если ваше антивирусное решение поддерживает защиту платежных онлайн-транзакций, убедитесь, что эта функция включена, прежде чем совершать покупку.

9. Регулярная проверка банковских выписок

Если вы стали жертвой киберпреступления, важно как можно скорее это обнаружить. Регулярно просматривайте историю операций и уточняйте у банка информацию по любым подозрительным транзакциям. Сотрудники банка смогут провести расследование и определить, является ли операция мошеннической.