



Санкт-Петербургский
государственный
университет
www.spbu.ru

Санкт-Петербургский государственный университет
Юридическая клиника

«Информационная безопасность»



Что такое информационная безопасность?

Информационная безопасность — это состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.



Для чего необходима информационная безопасность?

- Защитить граждан от информационных угроз.
- Реализовать конституционные права и свободы.
- Обеспечить достойные качество и уровень жизни граждан.
- Обеспечить безопасность жизни в государстве (как следствие безопасности государства от информационных угроз).



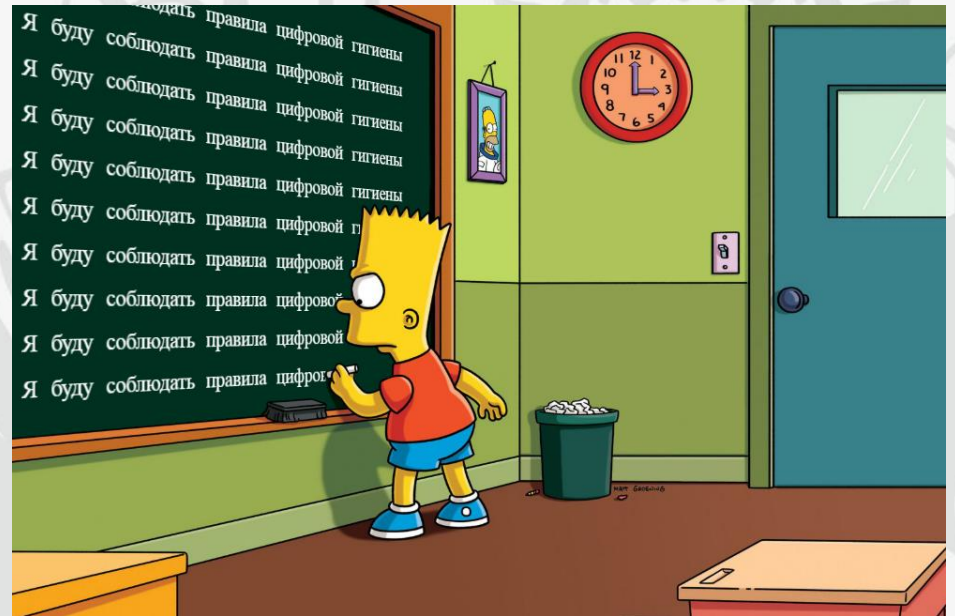
Важность информационной безопасности

Почему в понятии объединяется защищенность личности и государства? Ответ заключается в том, что ИБ подразумевает защищенность только в том случае, когда защищены все 3 субъекта — личность, общество и государство. В ином случае, уязвимость одного субъекта влечет к поражению другого элемента. Примерно, как эффект домино.





Соблюдение «цифровой гигиены» позволяет гражданам обезопасить себя в Интернете, а государству в лице органов и должностных лиц эффективно защищать права граждан, минимизировать ущерб, причиняемый правонарушениями в сети.





Правила «цифровой гигиены»

1. Не давайте свой телефон незнакомым людям, чтобы в руки мошенников не попали ваши персональные данные?
2. Используйте длинные и надежные пароли, а также биометрию и двухфакторную аутентификацию, особенно для платежей и денежных переводов. Использование удобных коротких паролей небезопасно.
3. Меньше рассказывайте о себе в интернете. Злоумышленники могут использовать раскрытые вашими же руками личные данные, чтобы атаковать вас.



4. Не принимайте запросы на дружбу от незнакомых людей в социальных сетях.
5. Следите за тем, какие приложения получают на ваших устройствах доступ и к чему. Новой игре совершенно не обязательно знать, где вы сейчас находитесь или иметь доступ к камере или микрофону.
6. Обновляйте программы и операционные системы на всех устройствах (не только мобильных). Разработчики в новых версиях добавляют не только красивые кнопки, но и закрывают уязвимости.



7. С осторожностью открывайте электронные письма с неизвестных адресов, чтобы избежать заражения.
8. Аккуратнее относитесь к использованию публичных сетей Wi-Fi при обращении к своему мобильному банку. В сети гостиниц и других мест отдыха часто внедряются любители легкой наживы.
9. Не скачивайте программное обеспечение с неизвестных сайтов.
10. Контролируйте, что ваш ребенок покупает в интернете — все средства для этого встроены в современные операционные системы. Только вы сами должны давать ребенку разрешение на покупку в сети. Заведите для этих целей отдельную дебетовую карту и пополняйте ее на ту сумму, которую не боитесь потерять.



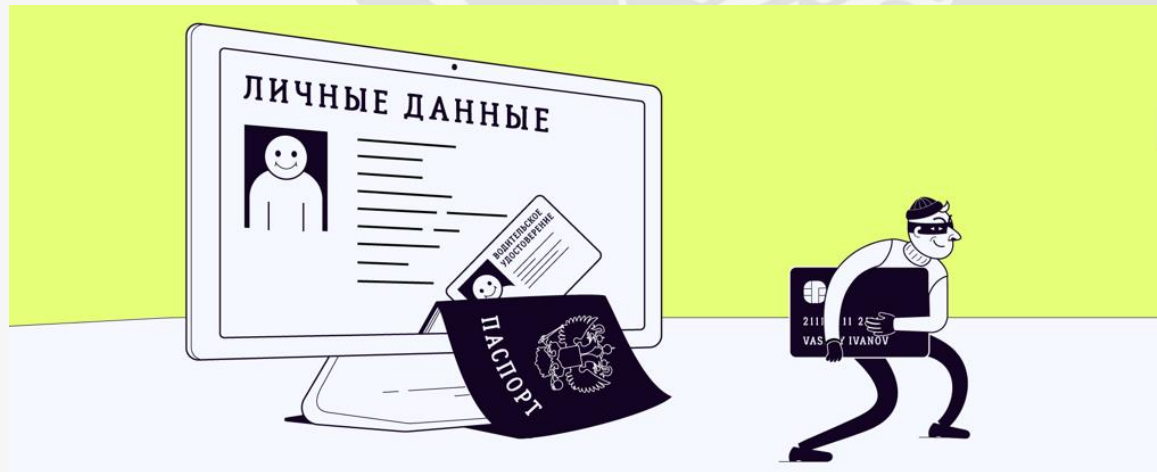
Информационная безопасность и «цифровая гигиена» взаимосвязаны и способствуют вашей защите!

Помните, что преступники не склонны ко взлому электронных систем ввиду сложности процесса. Для них удобнее всего воспользоваться доверчивостью людей, чтобы получить доступ к средствам интернет-банка или совершить от чужого имени противоправные действия





Противоправная деятельность в Интернете также лежит в рамках гражданской, административной и уголовной ответственности. Не стоит думать, что противоправные действия в Интернете не могут быть наказуемы по нормам Кодекса об административных правонарушениях РФ или Уголовного кодекса РФ.





Административная ответственность

Административным правонарушением признается противоправное, виновное действие (бездействие) физического или юридического лица, за которое КоАП или законами субъектов Российской Федерации об административных правонарушениях установлена административная ответственность».





Административная ответственность

Возраст привлечения к административной ответственности наступает с 16-ти лет. Однако не нужно думать, что до возраста 16-ти лет правонарушение останется безнаказанным.

Совершенные несовершеннолетними административные правонарушения могут повлечь привлечение к ответственности родителей или законных представителей по ст. 5.35 КоАП РФ «неисполнение родителями или иными законными представителями несовершеннолетних обязанностей по содержанию и воспитанию несовершеннолетних».



Некоторые составы правонарушений по КоАП РФ относятся в том числе и к деятельности людей в сети Интернет, например:

- Статья 6.21. Пропаганда нетрадиционных сексуальных отношений среди несовершеннолетних;
- Статья 13.15. Злоупотребление свободой массовой информации;
- Статья 13.18. Воспрепятствование уверенному приему радио- и телепрограмм и работе сайтов в сети «Интернет» (DDOS-атаки);
- Статья 20.1. Мелкое хулиганство;
- Статья 20.3.1. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства.



Административная ответственность

Действительно ли «троллинг» кого-либо в Интернете стоит того, чтобы оказаться наказанным?

Не стоит вступать в агрессивные споры в Интернете, либо заниматься травлей кого-либо. Лучше проигнорировать глупое замечание и заблокировать источник беспокойства.





Возможные виды административных наказаний по ст. 3.2. КоАП РФ по указанным составам административных правонарушений:

- административный штраф;
- конфискация предмета административного правонарушения;
- обязательные работы;
- административный арест (не применяется к несовершеннолетним).

Особенность применения административного штрафа в качестве вида наказания закреплена в ч.2 ст. 32.2 КоАП РФ и выражается в том, что в случае отсутствия у несовершеннолетнего самостоятельного заработка, сумма штрафа взыскивается с его родителей.



В соответствии со статьей 14 Уголовного кодекса РФ:
Преступление — это **виновно совершенное общественно опасное деяние, запрещенное Уголовным кодексом под угрозой наказания.**





Возраст привлечения к уголовной ответственности наступает с 16 лет. При этом есть особенности назначения наказания несовершеннолетним преступникам.

Однако, по некоторым составам преступлений ответственность наступает с 14 лет. Не все виды указанных преступлений возможно совершить с помощью Интернета, поэтому перечислим лишь некоторые:

- вымогательство (статья 163);
- прохождение обучения в целях осуществления террористической деятельности (статья 205.3);
- участие в террористическом сообществе (часть вторая статьи 205.4);
- заведомо ложное сообщение об акте терроризма (статья 207);
- незаконные приобретение, передачу, сбыт, хранение, перевозку или ношение взрывчатых веществ или взрывных устройств (статья 222.1).



Некоторые составы правонарушений по УК РФ могут быть связаны с деятельностью людей в сети Интернет, например:

- Статья 110. Доведение до самоубийства;
- Статья 151.2. Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего;
- Статья 205.2. Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма;
- Статья 245. Жестокое обращение с животными;
- Статья 280. Публичные призывы к осуществлению экстремистской деятельности.



Возможные виды уголовной ответственности по ст. 88 УК РФ по указанным составам преступлений:

- лишение свободы на определенный срок;
- ограничение свободы;
- штраф;
- обязательные работы;
- исправительные работы;
- лишение права заниматься определенной деятельностью.

Стоит подумать, прежде чем присоединяться к троллингу в интернете, ставить «лайк» или делиться результатами деструктивной деятельности других людей.



Сложилась судебная практика по статьям за «репосты». Стоит помнить, что администрации соцсетей активно сотрудничают с правоохранителями: могут предоставить информацию о времени и устройстве входа, его местоположении. Также сообщается, на кого зарегистрирована страница. Правоохранительные органы могут точно установить личность автора публикации.

ПАМЯТКА «РЕПОСТНЫЕ» СТАТЬИ

СТАТЬЯ 280

ПУБЛИЧНЫЕ ПРИЗЫВЫ К ОСУЩЕСТВЛЕНИЮ ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ
ЧАСТЬ ВТОРАЯ: ПУБЛИЧНЫЕ ПРИЗЫВЫ К ОСУЩЕСТВЛЕНИЮ ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ В ИНТЕРНЕТЕ



до 5 лет

до 3 лет

ИЛИ

до 5 лет

до 3 лет

СТАТЬЯ 282

ВОЗБУЖДЕНИЕ НЕНАВИСТИ ЛИБО ВРАЖДЫ, А РАВНО УНИЖЕНИЕ ЧЕЛОВЕЧЕСКОГО ДОСТОИНСТВА
ЧАСТЬ ПЕРВАЯ: ВОЗБУЖДЕНИЕ НЕНАВИСТИ И ВРАЖДЫ ПО РАСОВЫМ И ДРУГИМ ПРИЗНАКАМ В ИНТЕРНЕТЕ



300 000 до
500 000 руб

ИЛИ

1-4 года

ИЛИ

2 до 5 лет

СТАТЬЯ 282.1

ОРГАНИЗАЦИЯ ЭКСТРЕМИСТСКОГО СООБЩЕСТВА
ЧАСТЬ ВТОРАЯ: УЧАСТИЕ В ЭКСТРЕМИСТСКОМ СООБЩЕСТВЕ



300 000 до
600 000 руб

ИЛИ

1-4 года

ИЛИ

до 3 лет

ИЛИ

от 2 до 6 лет

до 5 лет

СТАТЬЯ 148

НАРУШЕНИЕ ПРАВА НА СВОБОДУ СОВЕСТИ И ВЕРОИСПОВЕДАНИЯ



300 000 руб

ИЛИ

до 240 часов

ИЛИ

до 1 года

ИЛИ

до 1 года

СТАТЬЯ 354

ПУБЛИЧНЫЕ ПРИЗЫВЫ К РАЗВЪЗЫВАНИЮ АГРЕССИВНОЙ ВОЙНЫ
ЧАСТЬ ПЕРВАЯ: ПРИЗЫВЫ К РАЗВЪЗЫВАНИЮ АГРЕССИВНОЙ ВОЙНЫ



300 000 руб

ИЛИ

до 3 лет



ШТРАФ



ПРИНУДИТЕЛЬНЫЕ/
ОБЯЗАТЕЛЬНЫЕ
РАБОТЫ



ЛИШЕНИЕ СВОБОДЫ



ЛИШЕНИЕ ПРАВА ЗАНИМАТЬ
ОПРЕДЕЛЕННЫЕ ДОЛЖНОСТИ



Помните! Даже если вы сами не писали провокационный комментарий, но он был написан от Вашего имени, то вас тоже могут привлечь к ответственности. Поэтому «цифровая гигиена» очень важна.

Легкомысленное обращение со своими персональными данными (паролями) делает вас и ваши персональные данные орудием в руках настоящих преступников.





Чтобы обезопасить себя, своих близких или знакомых, можно установить специальные фильтры.

Деструктивные материалы, а также небезопасные сайты пропадут из контента.



- Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
- Уголовный кодекс Российской Федерации» от 13.06.1996 № 63–ФЗ;
- Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195–ФЗ;
- <https://www.forbes.ru/forbes-woman/395719-cifrovaya-gigiena-pravila-informacionnoy-bezopasnosti-kotorym-stoit-nauchit>;
- <https://pravo.ru/story/204420/>;
- Канунникова Н.Г. Административная ответственность несовершеннолетних в Российской Федерации // Административное право и процесс. 2019. № 4. С. 48–50.