

ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Октябрь, 2022

В сфере информационной безопасности планируется сформировать информационное пространство для реализации творческих возможностей, доступности историко-культурного наследия, социализации молодёжи, а также обеспечить снижение уровня противоправного и преступного поведения среди детей и формирования у детей уважительного отношения к интеллектуальной собственности и авторскому праву, сознательный отказ от использования “пиратского контента”.



1. НОРМАТИВНАЯ БАЗА

Национальное законодательство Республики Беларусь в информационной сфере призвано регулировать общественные отношения, связанные с созданием, обработкой, предоставлением и защитой информации.

Нормы, касающиеся охраны и защиты прав на информацию, содержатся в специальных нормативно-правовых актах и частично в законах в различных сферах, где требуется документальное подтверждение каких-либо отношений к информации.

Документы в области информационной безопасности:

Вопросы информационной безопасности Республики Беларусь регулируются документами:

[Государственная программа «Цифровое развитие Беларуси на 2021-2025 годы»](#)

[Стратегия развития информатизации в Республике Беларусь на 2016-2022 годы](#)

Постановление Совета Безопасности Республики Беларусь № 1 от 18.03.2019 «О Концепции информационной безопасности Республики Беларусь»

Национальная стратегии устойчивого социально-экономического развития Республики Беларусь до 2030 года

Постановление Совета Безопасности Республики Беларусь [от 29 января 2021 г. № 57 О Государственной программе «Образование и молодежная политика» на 2021–2025 годы](#)

Закон Республики Беларусь от 7 мая 2021 г. № 99-3 "О защите персональных данных"

УКАЗ ПРЕЗИДЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ. 1 февраля 2010 г. № 60. О мерах по совершенствованию использования национального сегмента сети Интернет.

Законах Республики Беларусь от 10 ноября 2008 г. № 455-3 «Об информации, информатизации и защите информации»

Конституция Республики Беларусь

гарантирует следующие права и свободы:

- ✓ право каждого на защиту информации о его личной жизни, тайну корреспонденции, телефонных и иных сообщений (статья 28);
- ✓ право каждого на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, общественных объединений, о политической, экономической и международной жизни, состоянии окружающей среды. ... возможность каждому ознакомиться с материалами, затрагивающими его права и законные интересы (статья 34);
- ✓ свободу научного, технического творчества и охрану интеллектуальной собственности (статья 51);
- ✓ право собственности (статья 44)

Уголовный кодекс Республики Беларусь

РАЗДЕЛ XII, ГЛАВА 31

Преступления против информационной безопасности

- ✓ Статья 349. Несанкционированный доступ к компьютерной информации;
- ✓ Статья 350. Уничтожение, блокирование или модификация компьютерной информации;
- ✓ Статья 352. Неправомерное завладение компьютерной информацией;
- ✓ Статья 354. Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств;
- ✓ Статья 355. Нарушение правил эксплуатации компьютерной системы или сети

Кодекс Республики Беларусь «Об административных правонарушениях»

ГЛАВА 23

Административные правонарушения в области связи и информации

- ✓ Статья 23.4. Несанкционированный доступ к компьютерной информации;
- ✓ Статья 23.6. Разглашение коммерческой или иной охраняемой законом тайны;
- ✓ Статья 23.7. Нарушение законодательства о защите персональных данных;
- ✓ Статья 23.8. Разглашение служебной тайны по неосторожности

Постановление Совета Безопасности Республики Беларусь от 18.03.2019 № 1 «О Концепции информационной безопасности Республики Беларусь»

Все большее беспокойство вызывает активное распространение в информационном пространстве фальсифицированной, недостоверной и запрещенной информации. Снижение критического отношения потребителей информации к «фейковым» сообщениям новостных ресурсов, в социальных сетях и на других онлайн-платформах создает предпосылки преднамеренного использования дезинформации для дестабилизации общественного сознания в политических, социально-опасных, иных подобных целях.

В связи с этим особое значение приобретает ответственное поведение всех участников информационных процессов, а также выработка общих правил коммуникации в информационном пространстве, основанных на признании идентичности прав и обязанностей в существующей реальности (физическом мире) и виртуальном пространстве

Закон Республики Беларусь от 7 мая 2021 г. № 99-З "О защите персональных данных"

Все большее беспокойство вызывает активное распространение в информационном пространстве фальсифицированной, недостоверной и запрещенной информации. Снижение критического отношения потребителей информации к «фейковым» сообщениям новостных ресурсов, в социальных сетях и на других онлайн-платформах создает предпосылки преднамеренного использования дезинформации для дестабилизации общественного сознания в политических, социально-опасных, иных подобных целях.

В связи с этим особое значение приобретает ответственное поведение всех участников информационных процессов, а также выработка общих правил коммуникации в информационном пространстве, основанных на признании идентичности прав и обязанностей в существующей реальности (физическом мире) и виртуальном пространстве

2. ПОНЯТИЕ «ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Виды информации в зависимости от категории доступа:

- ☐ **общедоступная информация;**
- ☐ **информация, распространение и (или) предоставление которой ограничено:**
 - информация о частной жизни физического лица и персональные данные;
 - сведения, составляющие государственные секреты;
 - служебная информация ограниченного распространения;
 - информация, составляющая коммерческую, профессиональную, банковскую и иную охраняемую законом тайну;
 - информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу;
 - иная информация, доступ к которой ограничен законодательными актами Республики Беларусь

- **Информационная безопасность** - состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере
- **Защита информации** – комплекс правовых, организационных и технических мер по обеспечению **целостности, конфиденциальности, доступности** и **сохранности** информации

Концепция информационной безопасности Республики Беларусь



ЦЕЛОСТНОСТЬ – актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения

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

ДОСТУПНОСТЬ – это возможность за приемлемое время получить требуемую информационную услугу или необходимую информацию

СОХРАННОСТЬ – при любых обстоятельствах данные не будут безвозвратно потеряны

Меры по защите информации

Организационные

- разработка внутренней документации;
- инструктажи и периодические проверки персонала, проведение тренингов по вопросам безопасности;
- разграничение зон ответственности;
- и другие.

Технические

- меры по физической недоступности объектов (замки, камеры, сигнализация, жалюзи);
- установка программного обеспечения для защиты информации от несанкционированного доступа;
- управление доступом, паролями и ресурсами;
- резервное копирование

Правовые

- соблюдение законодательства в информационной сфере

Цели нарушителей

- нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики.
- дискредитация или дестабилизация деятельности органов государственной власти, организаций;
- причинение имущественного ущерба путем мошенничества или иным преступным путем;
- получение конкурентных преимуществ - попытка нарушить конфиденциальность информации с целью похищения каких-то коммерческих секретов;
- любопытство или желание самореализации - это типичная цель для сотрудников организации, которые не хотят нанести серьезный ущерб, но стремятся самоутвердиться или самореализоваться, а стремясь достичь этой цели, могут нарушать безопасность информации и нанести ущерб информации;
- неквалифицированные действия сотрудников или действия по неосторожности, ошибки

11 Советов по Безопасности в Интернете (видео)



Масштаб потребительских киберугроз

Хотя 7 из 10 пользователей утверждают, что понимают риск киберугроз и знают как защитить себя онлайн...



пользователей хотя бы
2/3 раз в жизни
становились жертвами
киберпреступлений

1.5 миллиона
жертв кибератак в день



жертв в секунду

\$110 млрд

СОВОКУПНЫЙ УЩЕРБ
ОТ КИБЕРПРЕСТУП-
ЛЕНИЙ В ГОД



Киберпреступления в соц.сетях и мобильных платформах

Киберпреступники идут
в мобильные устройства

2/3

2/3 ПОЛЬЗОВАТЕЛЕЙ
ПОЛЬЗУЮТСЯ ИНТЕРНЕТОМ
ЧЕРЕЗ МОБИЛЬНЫЕ УСТРОЙСТВА

ПОЛЬЗОВАТЕЛЕЙ МОБИЛЬНЫХ
УСТРОЙСТВ

31%

Получали текстовые
сообщения от неизвестных
лиц с предложением
перейти по неизвестной
ссылке или набрать
незнакомый номер для
получения голосового
сообщения

ПОКА

2/3

НЕ ПОЛЬЗУЮТСЯ РЕШЕНИЯМИ
ПО БЕЗОПАСНОСТИ НА
МОБИЛЬНЫХ
УСТРОЙСТВАХ