

ПРАВОВЫЕ НОРМЫ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

ВЫПОЛНИЛА:

СТУДЕНТКА 1 КУРСА

ГРУППЫ №18

АМЕЛЬЧЕНКО ИРИНА

ПРЕПОДАВАТЕЛЬ:

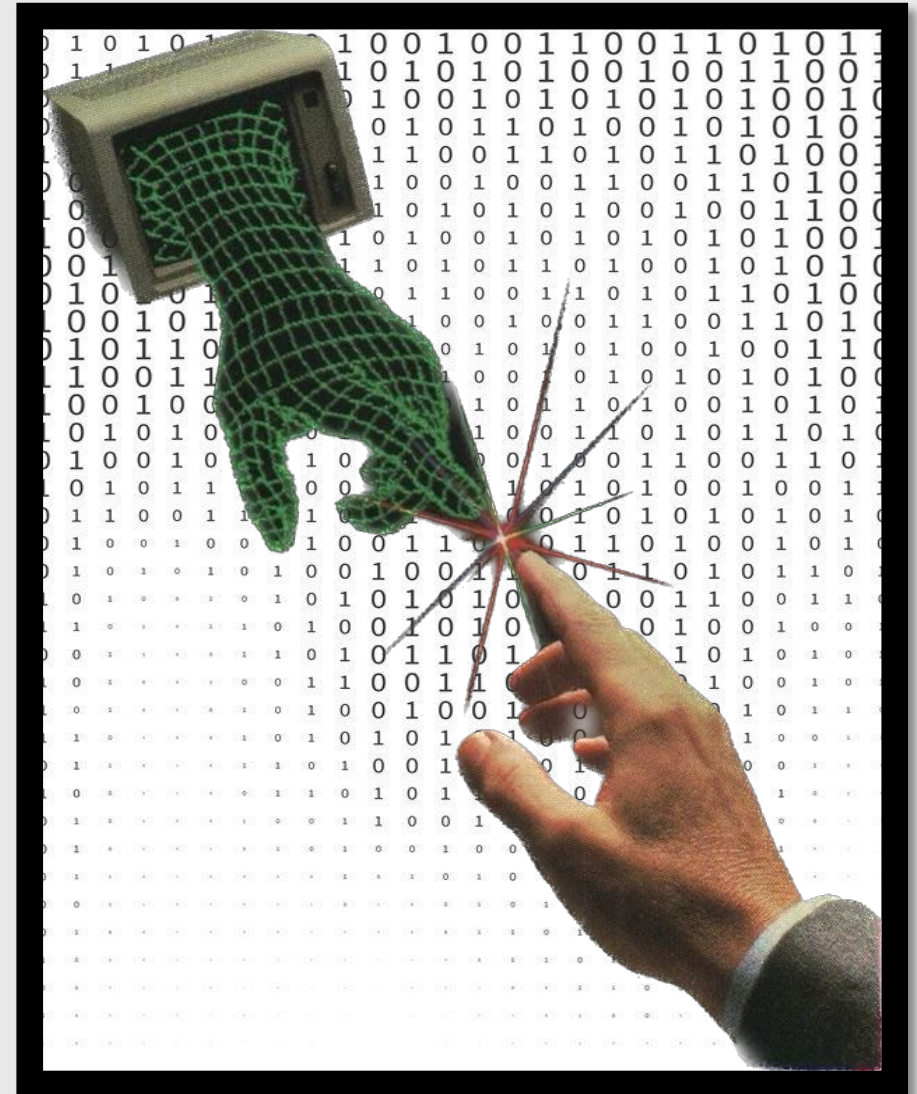
ОРЛОВА ТАТЬЯНА НИКОЛАЕВНА

САНКТ-ПЕТЕРБУРГ, 2022Г.

ИНФОРМАЦИЯ

Информация- это сведения (сообщения, данные) независимо от формы их представления;

Информация является объектом правового регулирования. Информация не является материальным объектом, но она фиксируется на материальных носителях. Первоначально информация находится в памяти человека, а затем она отчуждается и переносится на материальные носители: книги, диски и другие накопители, предназначенные для хранения информации



ИНФОРМАЦИОННО-ПРАВОВЫЕ НОРМЫ

Информационно-правовые нормы регулируют обособленную группу общественных отношений применительно к особенностям информационной сферы; задает содержание прав и обязанностей субъектов, участвующих в правоотношении. Информационно-правовые нормы регулируют взаимоотношения граждан, СМИ, организаций, фирм между собой, их взаимные права и обязанности.



ПРАВО СОБСТВЕННОСТИ

- Право распоряжения состоит в том, что только субъект-владелец информации имеет право определять, кому эта информация может быть предоставлена.
- Право владения должно обеспечивать субъекту-владельцу информации хранение информации в неизменном виде. Никто, кроме него, не может ее изменять.
- Право пользования предоставляет субъекту-владельцу информации право ее использования только в своих интересах.

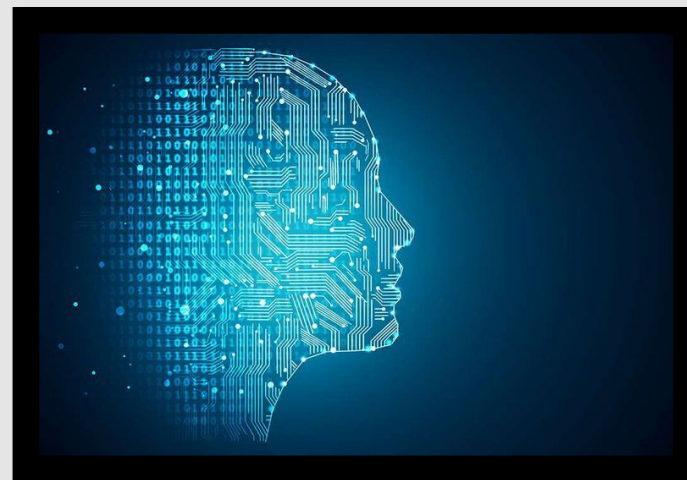


ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная безопасность Российской Федерации – это состояние защищенности её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

В связи с возрастающим значением информационных ресурсов предприняты ряд правовых мер для их охраны и защиты. Многие черты информационного общества уже присутствуют в современной жизни развитых стран. Жизненно важной для общества становится проблема информационной безопасности действующих систем хранения, передачи и обработки информации.

Более 80% компьютерных преступлений осуществляется через глобальную сеть Интернет, которая обеспечивает широкие возможности злоумышленникам для нарушений в глобальном масштабе.



ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В соответствии с действующим уголовным законодательством Российской Федерации под преступлениями в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

Неправомерный доступ к компьютерной информации (ст. 272 УК РФ), а также создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ) совершаются только путём действий, в то время как нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ) – путём как действий, так и бездействием.



МЕРЫ ПО ПРЕДУПРЕЖДЕНИЮ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

- Технические;
- Организационные;
- Правовые.



К ТЕХНИЧЕСКИМ МЕРАМ ОТНОСЯТ:

- защиту от несанкционированного доступа к системе,
- резервирование особо важных компьютерных подсистем,
- организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев,
- установку оборудования обнаружения и тушения пожара,
- оборудования обнаружения воды,
- принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания,
- оснащение помещений замками, установку сигнализации и многое другое.



К ОРГАНИЗАЦИОННЫМ МЕРАМ ОТНОСЯТ:

- охрану вычислительного центра,
- тщательный подбор персонала,
- исключение случаев ведения особо важных работ только одним человеком,
- наличие плана восстановления работоспособности центра после выхода его из строя,
- организацию обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра,
- универсальность средств защиты от всех пользователей (включая высшее руководство), возложение ответственности на лиц, которые должны обеспечить безопасность центра.



К ПРАВОВЫМ МЕРАМ ОТНОСЯТ:

- разработку норм, устанавливающих ответственность за компьютерные преступления,
- защита авторских прав программистов,
- совершенствование уголовного, гражданского законодательства и судопроизводства.
- общественный контроль за разработчиками компьютерных систем и принятие международных договоров об ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты жизни стран, заключающих соглашение.

