Информационная безопасность

Виды информационных угроз

Методы защиты информации

Информационная безопасность

Процесс информатизации неизбежно приводит к интеграции этих сред, поэтому проблему защиты информации необходимо решать, учитывая всю совокупность условий циркуляции информации, создания и использования информационных ресурсов в этой информационной среде.

Информационная среда — это совокупность условий, средств и методов на базе компьютерных систем, предназначенных для создания и использования информационных ресурсов.

Совокупность факторов, представляющих опасность для функционирования информационной среды, называют ***информационными угрозами***.

Информационная безопасность — совокупность мер по защите информационной среды общества и человека.

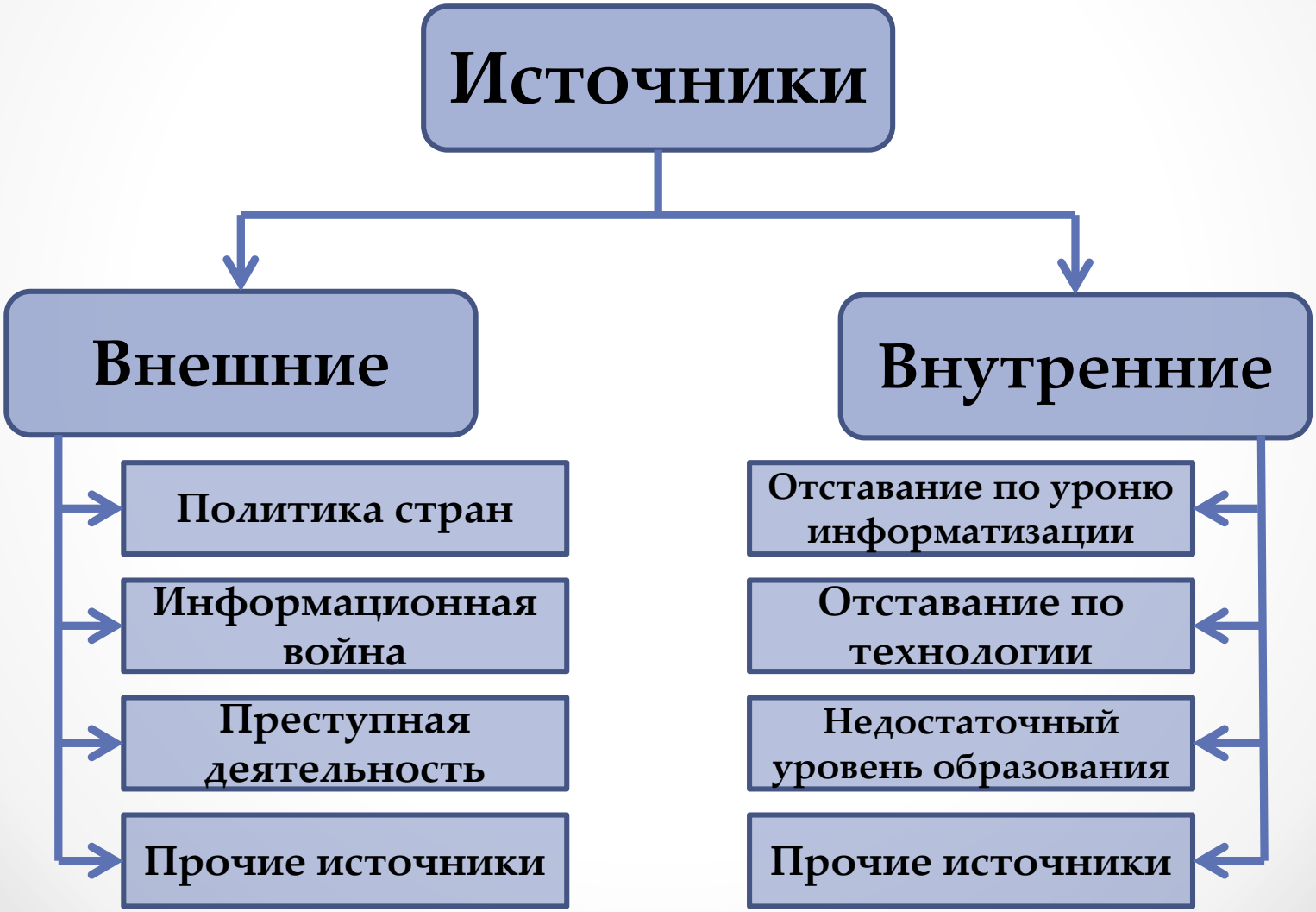
Цели информационной безопасности

- защита национальных интересов;
- обеспечение человека и общества достоверной и полной информацией;
- правовая защита человека и общества при получении, распространении и использовании информации.

Объекты обеспечения информационной безопасности

- информационные ресурсы;
- система создания, распространения и использования информационных ресурсов;
- информационная инфраструктура общества (информационные коммуникации, сети связи, центры анализа и обработки данных, системы и средства защиты информации);
- средства массовой информации;
- права человека и государства на получение, распространение и использование информации;
- защита интеллектуальной собственности и конфиденциальной информации.

Источники информационных угроз

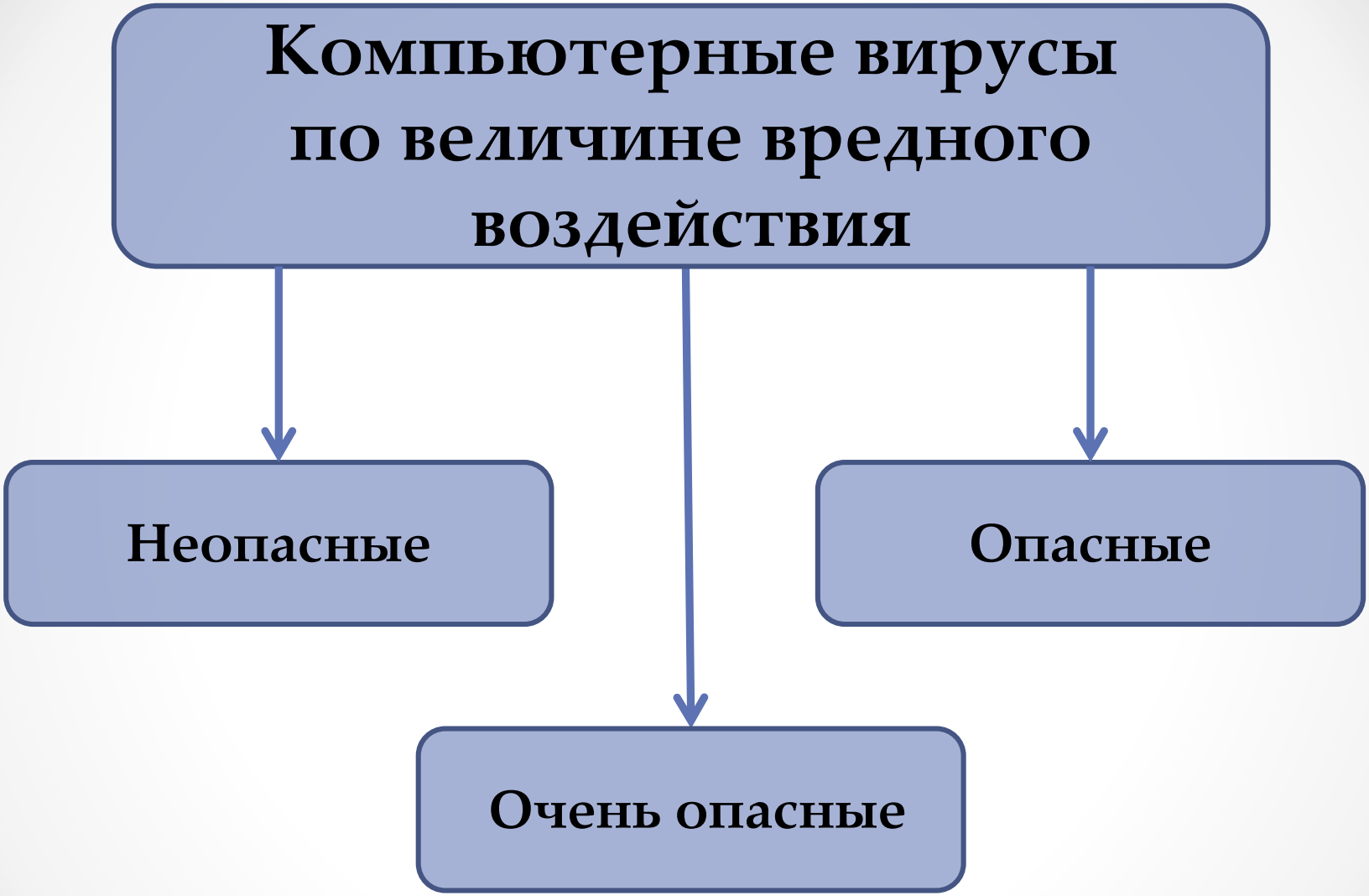


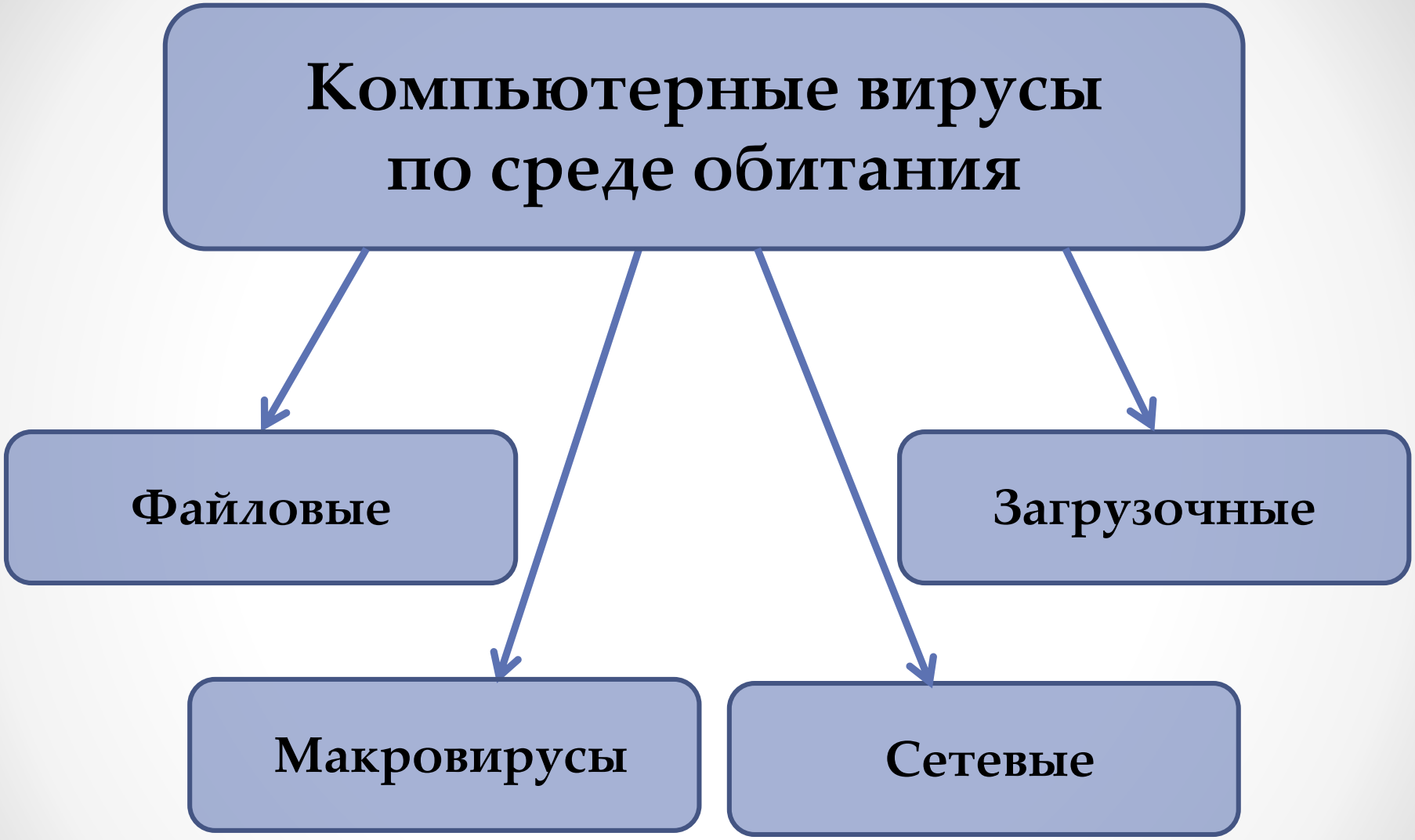
Виды информационных угроз

Компьютерные вирусы

Компьютерный вирус –

это небольшая программа, написанная программистом высокой квалификации, способная к саморазмножению и выполнению разных вредоносных действий.


Компьютерные вирусы по величине вредного воздействия
Неопасные
Очень опасные
Опасные


Компьютерные вирусы
по среде обитания
Файловые
Загрузочные
Макровирусы
Сетевые

Понятия и их определения

- **Компьютерная безопасность** меры безопасности, применяемые для защиты вычислительных устройств (компьютеры, смартфоны и другие), а также компьютерных сетей (частных и публичных сетей, включая Интернет.

- **Цифровая безопасность** представляет собой сочетание инструментов и привычек, которые пользователи могут использовать, во избежание контроля над их действиями в Интернете, доступа или вмешательства в их электронную информацию и вмешательства в их электронные устройства и программы.

- **Цифровая грамотность** - набор компетенций, связанных с квалифицированным использованием компьютеров и информационных технологий.

- **Цифровая гигиена** - это свод правил, следуя которым, человек обеспечивает себе информационную безопасность (не анонимность, а защиту) в сети Интернет. Относится к сфере знаний о цифровой безопасности.

Понятия и их определения

- **Кибербезопасность** - состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз.
- **Кибербуллинг** - это травля с использованием цифровых технологий.
- **Троллинг** — форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации.
- **Персональные данные** - основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами Республики Беларусь внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо.
- **Нежелательный контент** - это не только материалы (картинки, видео, аудио, тексты), содержащие насилие, порнографию, пропаганду наркотических средств, азартных игр, но и различные вредоносные и шпионские программы, задача которых получить доступ к информации на компьютере владельца. Также к нежелательному контенту относятся сайты, запрещенные законодательством.

Понятия и их определения

- **Фишинг** - вид мошенничества, цель которого является получение конфиденциальных данных для доступа к различным сервисам (электронной почте, интернет-банкингу и т.д.).
- **Вишинг** - это устная разновидность фишинга, при которой злоумышленники посредством телефонной связи, используя приемы, методы и технологии социальной инженерии, под разными предлогами, искусно играя определенную роль, вынуждают человека сообщить им свои конфиденциальные банковские или персональные данные либо стимулируют к совершению определенных действий со своим банковским счетом или банковской картой.
- **Смишинг** - вид мошенничества, целью которого является переход по ссылке из SMS и/или загрузки вредоносного программного обеспечения.
- **Сваттинг** - тактика домогательства, которая реализуется посредством направления ложного вызова той или иной службе. Например, люди сообщают о минированиях, преследуя цель устроить неразбериху и панику в конкретном месте.
- **Груминг** - это установление дружеского и эмоционального контакта с ребенком в Интернете для его дальнейшего совращения.

Нормативные документы

- Постановление Оперативно-аналитического центра при Президенте Республики Беларусь, Министерства связи и информатизации Республики Беларусь от 19 февраля 2015 года № 6/8 «Об утверждении Положения о порядке ограничения доступа к информационным ресурсам (их составным частям), размещенным в глобальной компьютерной сети Интернет»
- Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 года № 1 «О Концепции информационной безопасности Республики Беларусь»
- Закон Республики Беларусь от 19 ноября 1993 г. О правах ребенка Статья 37-2. «Меры по защите детей от информации, причиняющей вред их здоровью и развитию» Ссылка
- Постановление Совета Министров Республики Беларусь 29 января 2021 г. № 57 О Государственной программе «Образование и молодежная политика» на 2021-2025 годы.

Законодательство по киберпреступлениям

В Уголовном кодексе Республики Беларусь содержится ряд статей, предусматривающих уголовную ответственность за киберпреступления:

- ст.212 «Хищение путем использования компьютерной техники»;
- ст.349 «Несанкционированный доступ к компьютерной информации»;
- ст.350 «Модификация компьютерной информации»;
- ст.351 «Компьютерный саботаж»;
- ст.352 «Неправомерное завладение компьютерной информацией»;
- ст.353 «Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети»;
- ст.354 «Разработка, использование либо распространение вредоносных программ»;
- ст.355 «Нарушение правил эксплуатации компьютерной системы или сети»

Основные виды негативного контента

1) информация о способах и средствах совершения преступлений, иных правонарушений или антиобщественных действий, а также действий, опасных для жизни и здоровья человека;
2) сексуально откровенный контент и иная непристойная информация;
3) нецензурная брань;
4) контент устрашающего характера, включая изображение или описание насилия, жестокости, катастроф или несчастных случаев;
5) заведомо ложная информация;
6) дискредитирующая информация;
7) скрытая информация, воздействующая на подсознание человека;
8) реклама товаров и услуг, которые могут причинить вред жизни и здоровью человека.

Методы защиты информации

При разработке методов защиты информации в информационной среде следует учесть следующие важные факторы и условия:

- расширение областей использования компьютеров и увеличение темпа роста компьютерного парка;
- высокая степень концентрации информации в центрах ее обработки и, как следствие, появление централизованных баз данных, предназначенных для коллективного пользования;
- расширение доступа пользователя к мировым информационным ресурсам;
- усложнение программного обеспечения вычислительного процесса на компьютере.

Методы защиты:

- Ограничение доступа к информации;
- Шифрование информации;
- Контроль доступа к аппаратуре;
- Законодательные меры.

С каждым годом количество угроз информационной безопасности компьютерных систем и способов их реализации постоянно увеличивается. Основными причинами здесь являются недостатки современных информационных технологий и постоянно возрастающая сложность аппаратной части. На преодоление этих причин направлены усилия многочисленных разработчиков программных и аппаратных методов защиты ин-формации в компьютерных системах.

Политика безопасности

Политика безопасности —

это совокупность технических, программных и организационных мер, направленных на защиту информации в компьютерной сети.