Лекция №7
«Информационная безопасность»

Специальность 31.02.01 «Лечебное дело»

1. Информационная безопасность

Под **информационной безопасностью** понимается состояние защищенности информационной среды общества, обеспечивающее ее формирование и развитие в интересах граждан, организаций и государства.

Суть информационной безопасности состоит в проведении правовых, организационных и технических мероприятий при формировании и использовании информационных технологий, инфраструктуры и информационных ресурсов, защите информации и прав субъектов, участвующих в информационной деятельности.

Важнейшими задачами обеспечения информационной безопасности Российской Федерации являются:

реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности;

совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство; противодействие угрозе развязывания противоборства в информационной сфере.

Субъекты ИБ:

- органы государственной власти;
- средства массовой информации;
- граждане и общественные объединения;
- предприятия и организации независимо от

формы собственности.

Угрозы ИБ:

- информационная война;
- деятельность разведывательных и специальных служб иностранных государств;
- деятельность иностранных негосударственных структур и организаций, несовместимая с безопасностью и интересами государства;
- преступные действия иностранных и международных криминальных групп, структур и отдельных лиц;
- противозаконная деятельность юридических и физических лиц, а также иных субъектов в области формирования, использования и распространения информации, включая нарушение установленных регламентов сбора и использования информации.

2. За что отвечает информационная безопасность

Она отвечает за три группы проблем:

нарушение конфиденциальности информации

- это – разглашение или утечка какой-либо информации, не предназначенной для третьих лиц, без согласия на то ее обладателя

нарушение целостности информации

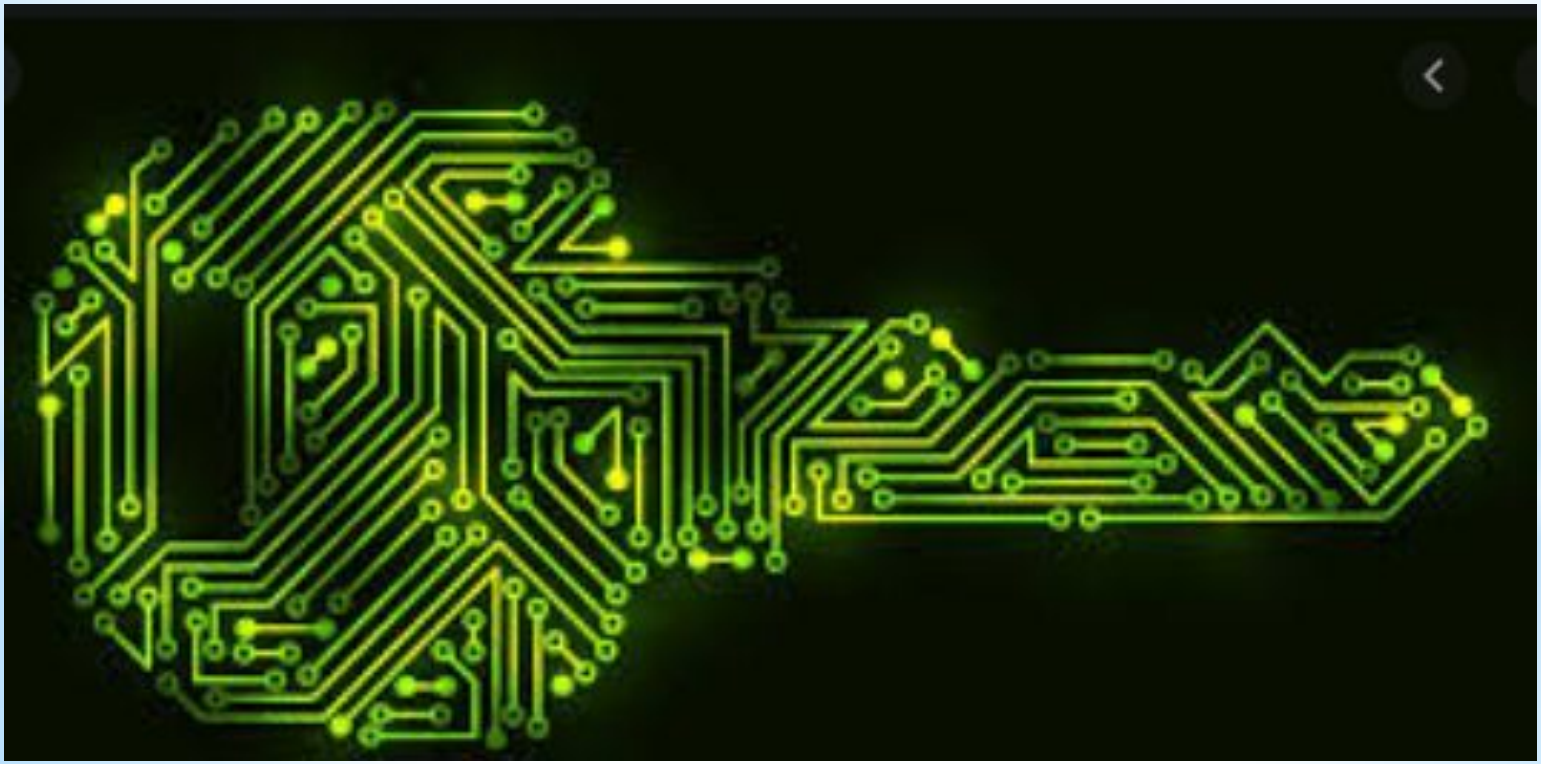
- это – изменение данных при хранении, обработке и передачи информации, т.е. сохранение данных в том виде, в каком они были созданы

нарушение доступности

- означает, что тот, кто имеет право на доступ к информации, может ее получить. Например, вы в любой момент можете войти в свою электронную почту. Если хакеры атакуют серверы, почта будет недоступна, это нарушит доступность.

3.Основные понятия

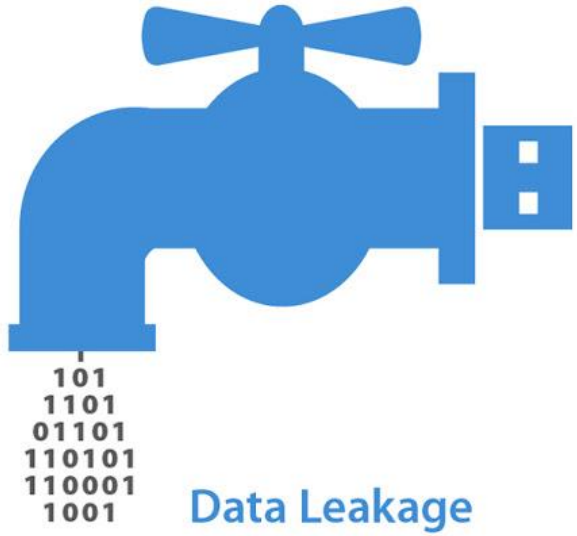
* **Защита информации** — это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.



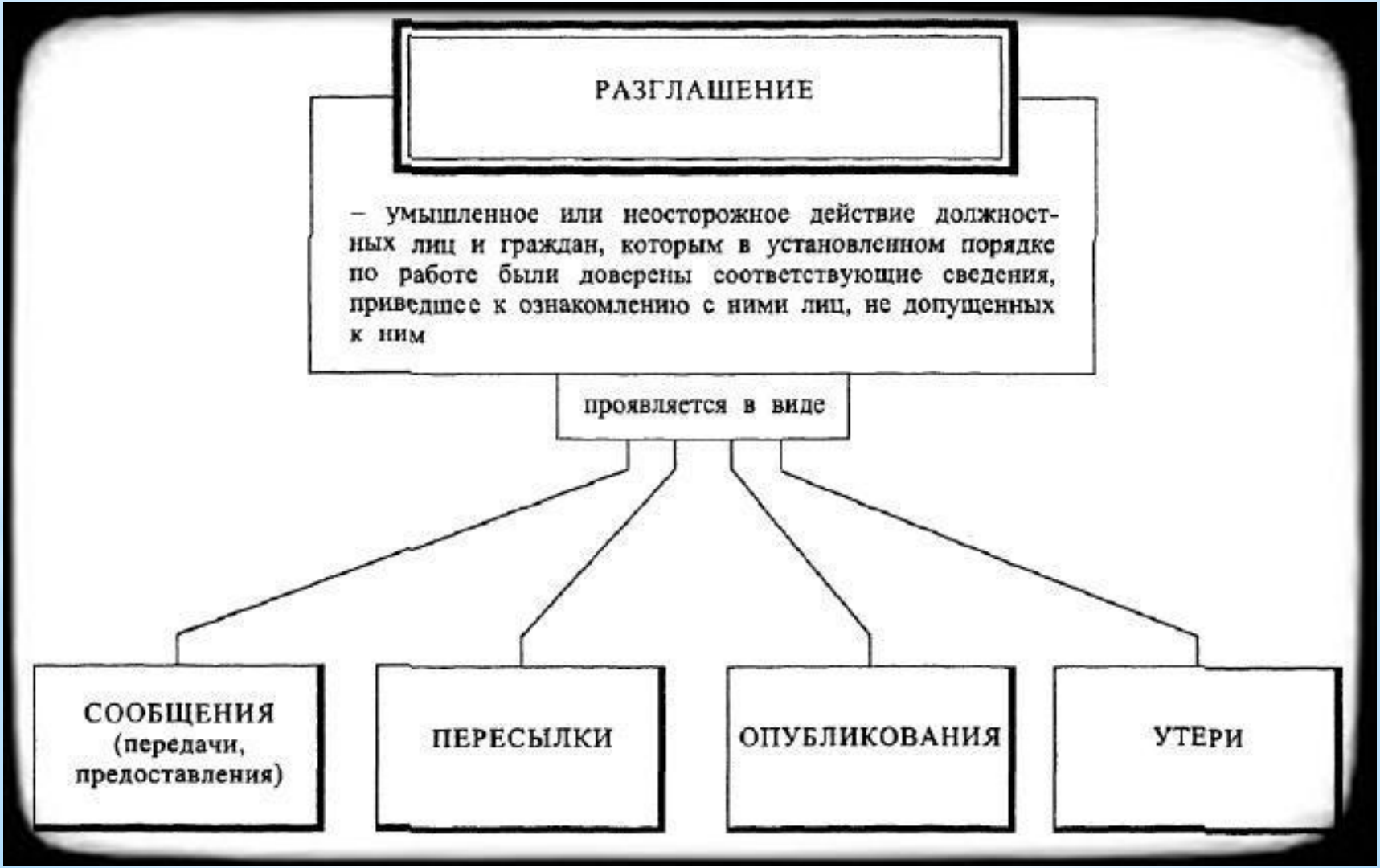
* **Объект защиты** — информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

* **Цель защиты информации** —предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

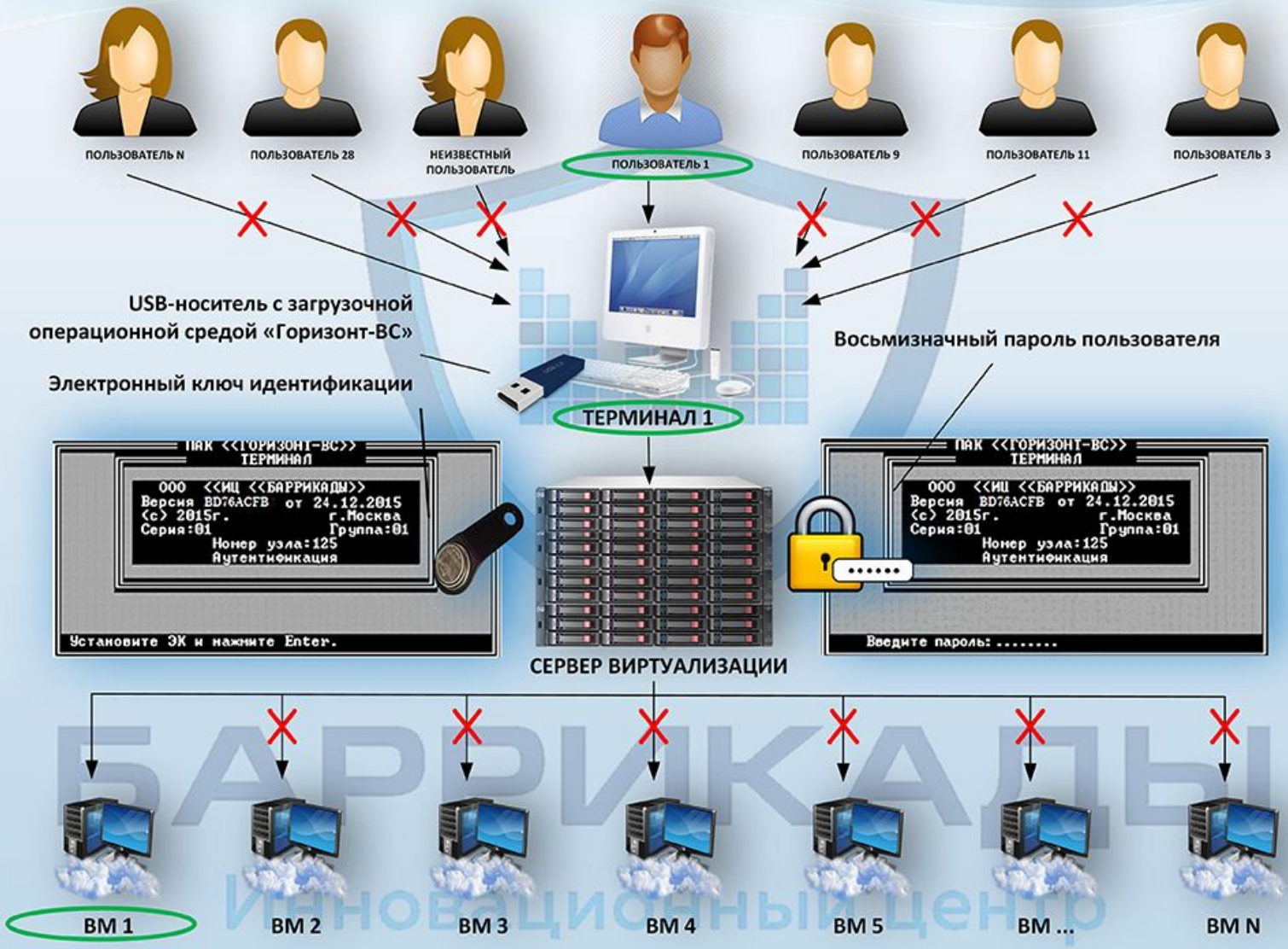
Защита информации от утечки — деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.



* **Защита информации от разглашения** — деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.



Защита от несанкционированного доступа в доверенной среде ПАК «Горизонт-ВС»

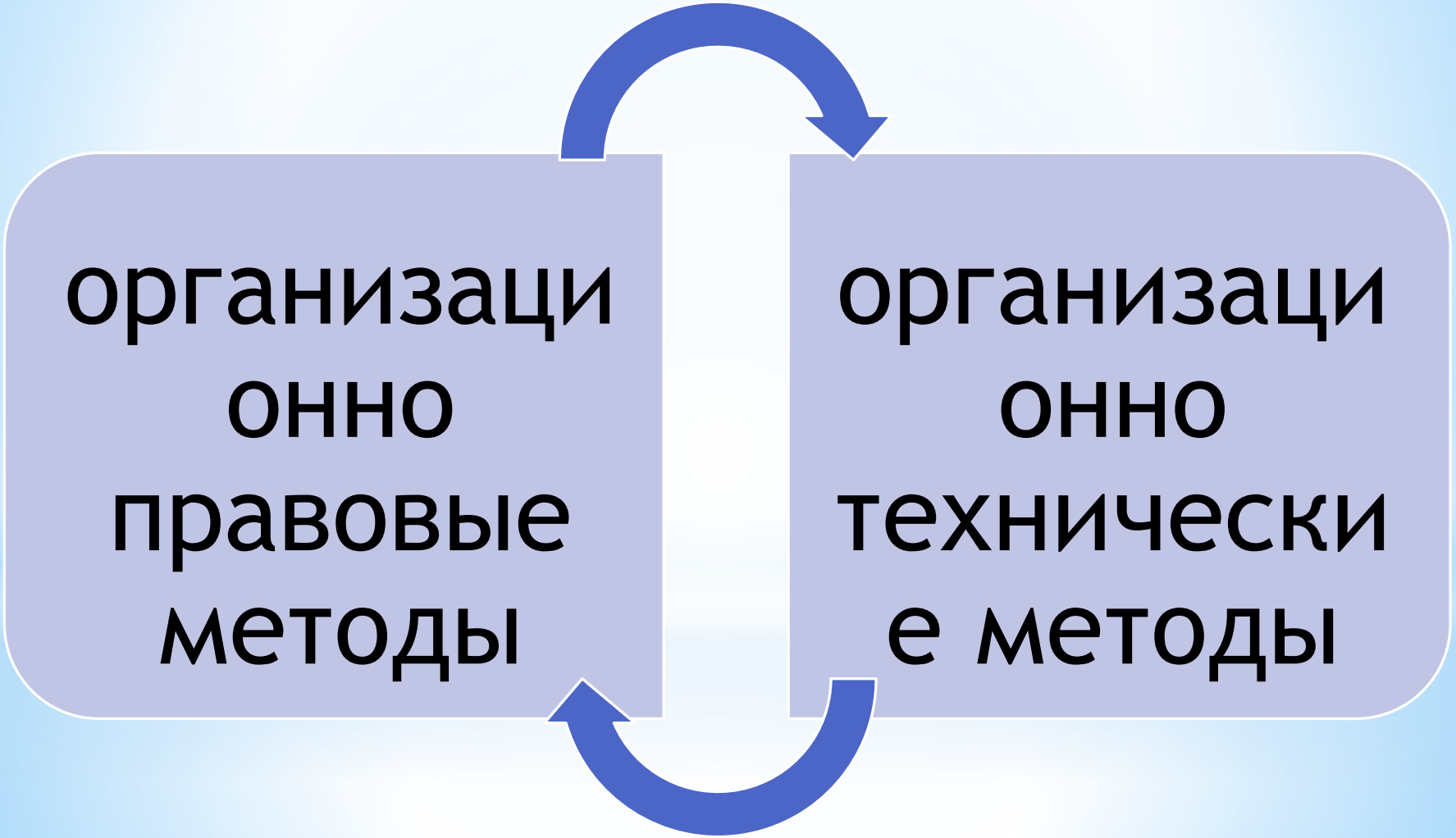


* **Защита информации от НСД** — деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации.

* **Информационная безопасность** - защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности.

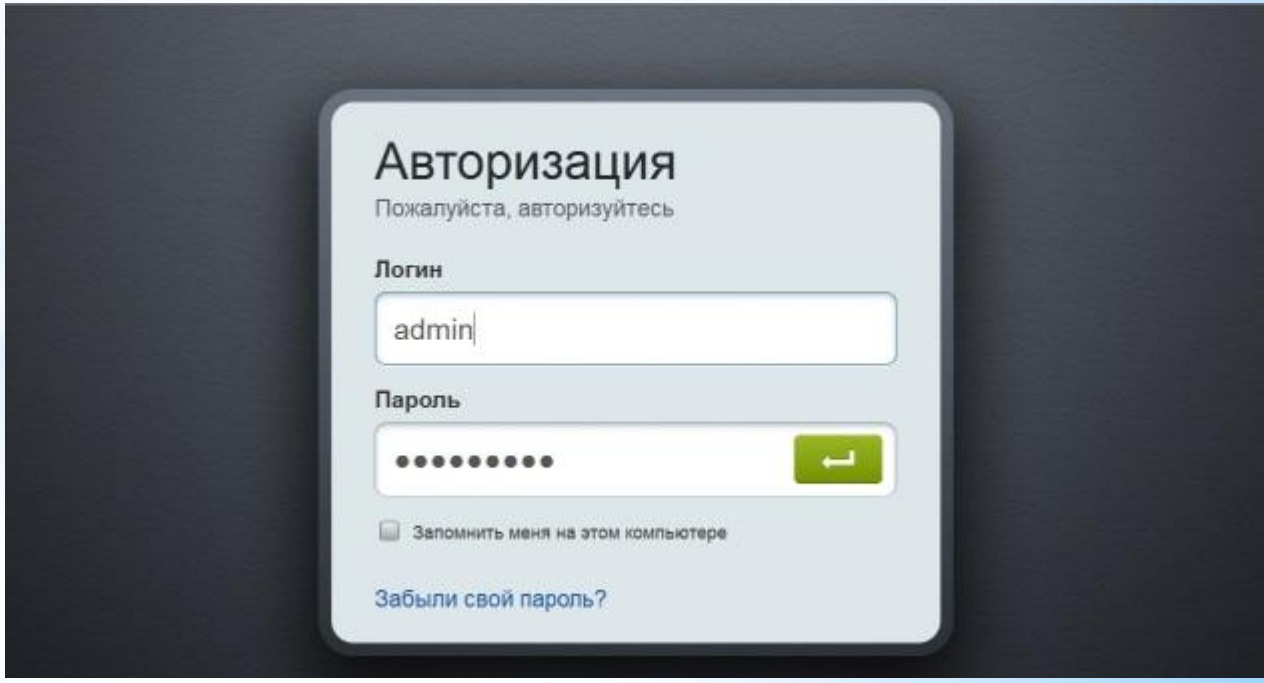
4.Методы защиты информации

Методы защиты информации:



*Авторизация.

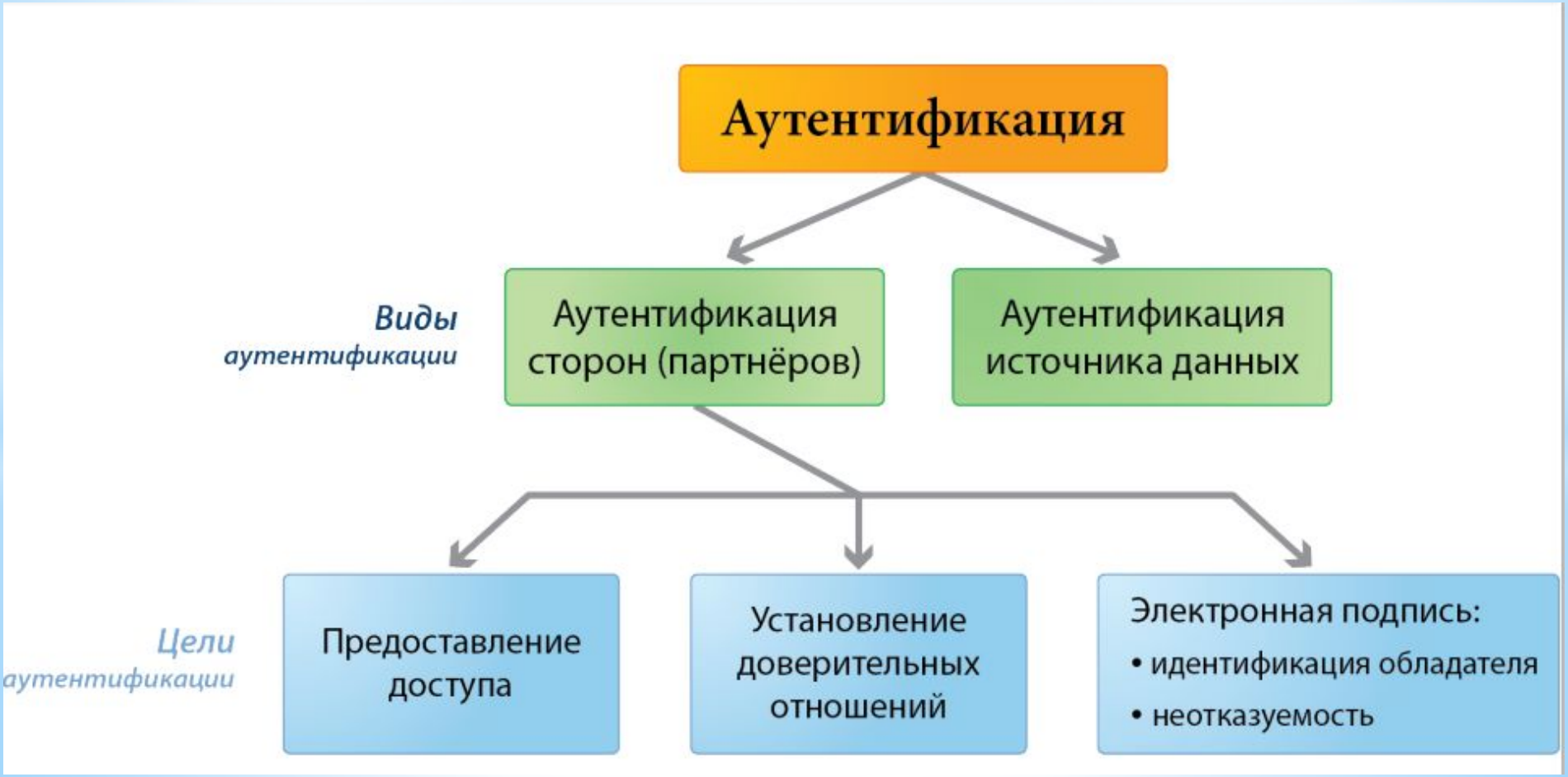
Этот метод позволяет создавать группы пользователей, наделять эти группы разными уровнями доступа к сетевым и информационным ресурсам и контролировать доступ пользователя к этим ресурсам.



*Идентификация

Идентификация позволяет определить субъект (терминал пользователя, процесс) по уникальному номеру, сетевому имени и другим признакам.

* **Аутентификация**- проверка подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д.



Методы аутентификации

* **Биометрия**. Используется аутентификация по геометрии руки, радужной оболочке сетчатки глаза, клавиатурный почерк, отпечатки глаза и т.п.

ПОРЯДОК ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ МЕССЕНДЖЕРОВ

УСТАНАВЛИВАЕТ ПРИЛОЖЕНИЕ

УКАЗЫВАЕТ НОМЕР ТЕЛЕФОНА В МЕССЕНДЖЕРЕ

ОТПРАВЛЯЕТ ЗАПРОС ОПЕРАТОРУ

СВЕРЯЕТ НОМЕР СО СВОЕЙ АБОНЕНТСКОЙ БАЗОЙ

В ТЕЧЕНИЕ 20 МИНУТ ОТПРАВЛЯЕТ ОТВЕТ МЕССЕНДЖЕРУ О НАЛИЧИИ ИЛИ ОТСУТСТВИИ СВЕДЕНИЙ ОБ АБОНЕНТЕ В СВОЕЙ БАЗЕ

ДА

ОТПРАВЛЯЕТ ОПЕРАТОРУ УНИКАЛЬНЫЙ ИДЕНТИФИКАЦИОННЫЙ КОД ПОЛЬЗОВАТЕЛЯ

НЕТ

ОТКАЗЫВАЕТ ПОЛЬЗОВАТЕЛЮ В УСЛУГЕ

ВНОСИТ В БАЗУ ДАННЫХ НАЗВАНИЕ МЕССЕНДЖЕРА И УНИКАЛЬНЫЙ ИДЕНТИФИКАЦИОННЫЙ КОД ПОЛЬЗОВАТЕЛЯ

ПОЛЬЗОВАТЕЛЬ

МЕССЕНДЖЕР

ОПЕРАТОР

Физическая защита.

Физические средства защиты — разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников.К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа-выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий.

Эти средства применяются для решения следующих задач:

1. охрана территории предприятия и наблюдение за ней;
2. охрана зданий, внутренних помещений и контроль за ними;
3. охрана оборудования, продукции, финансов и информации;
4. осуществление контролируемого доступа в здания и помещения.

* **SMART-карты** (интеллектуальные карты). Их удобство заключается в портативном и широком спектре функций, которые могут быть легко модифицированы.

e-Token (электронный ключ) – аналог SMART-карты, выполненный в виде брелка, подключающегося через USB-порт.

Меры по защите информации и сетей осуществляются в России нормами закона «Об информации, информационных технологиях и о защите информации»

Закон РФ №149-ФЗ регулирует отношения, возникающие при: осуществлении права на поиск, получение, передачу и производство информации; применении информационных технологий; обеспечении защиты информации.

В частности, в статье 8 «Право на доступ к информации» утверждается право гражданина на получение из официальных источников информации о деятельности государственных органов, об использовании бюджетных средств, о состоянии окружающей среды, и пр., а также любой информации, непосредственно затрагивающей его права и свободы. Ограничение доступа к информации устанавливается только федеральными законами, направленными на обеспечение государственной безопасности.

В статье 12 «Государственное регулирование в сфере применения информационных технологий», в частности, отмечается, что обязанностью государства является создание условий для эффективного использования в Российский Федерации информационно-телекоммуникационных сетей, в том числе Интернета.

Особое внимание обратим на статью 3, в которой среди принципов правового регулирования в информационной сфере провозглашается принцип неприкосновенности частной жизни, недопустимость сбора, хранения использования и распространения информации о частной жизни лица без его согласия.

* В 2006 году вступил в силу **закон №152-0ФЗ «О персональных данных»**, целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных (с использованием средств автоматизации или без использования таких), в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

* В современном информационном обществе информация является товаром. Производство программ и информационных ресурсов ведется в индустриальных масштабах, над ними работают коллективы профессиональных программистов. Основой правовых отношений между пользователем и собственником программного обеспечения является ***лицензия*** — это документ, определяющий порядок использования и распространения программного обеспечения, защищённого авторским правом.

* Производимые программные продукты по условиям распространения можно разделить на четыре группы: лицензируемые; условно бесплатные (shareware, trial, демо); распространяемые бесплатно (freeware) и распространяемые свободно в виде исходных кодов (free software). Форма, в которой распространяется программный продукт, называется его ***дистрибутивом***. Дистрибутивы ***лицензируемых*** программ распространяются фирмой-продавцом на основании договора с покупателем на платной основе.

* Проблемы информационной безопасности в России регламентируются **Доктриной информационной безопасности Российской Федерации**, согласно которой под информационной безопасностью Российской Федерации понимается состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

В доктрине выделены четыре основные составляющие национальных интересов Российской Федерации в информационной сфере:

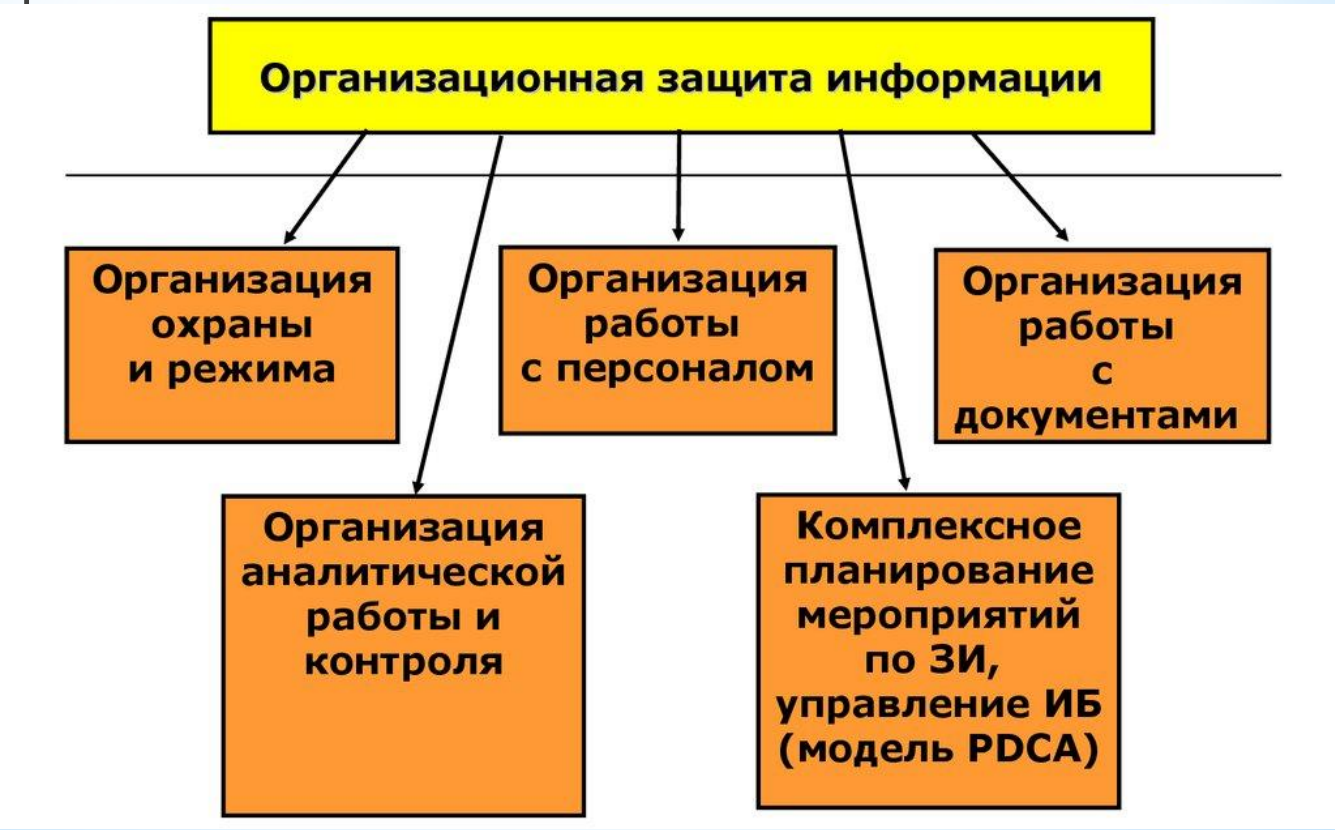
* соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею;
* обеспечение духовного обновления России; сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;

* информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, её официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам;
* развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи; обеспечение потребностей внутреннего рынка её продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;
* защита информационных ресурсов от несанкционированного доступа;
* обеспечение безопасности информационных и телекоммуникационных систем, как уже развёрнутых, так и создаваемых на территории России.

В современной практике выделяют следующие группы средств:

* организационные;
* антивирусные;
* защита с помощью паролей;
* криптографические;
* стенографические.

* **Организационные методы** создаются в каждой организации в соответствии с требованиями и условиями ее деятельности, в результате чего, в фирме имеются специфические способы и нормы защиты.



* Защита информации организационными средствами предполагает защиту без использования технических средств.

Защита информации — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

* Различают **несанкционированное** и **непреднамеренное** воздействие на информацию.

* **Несанкционированным** является воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации. Такого рода воздействие на информацию или ресурсы информационной системы может осуществляться с помощью вредоносных программ (вирусов).

Так же информация может быть утеряна, искажена или блокирована **непреднамеренно**, например, из-за ошибочного действия пользователя или сбоя оборудования. Для предотвращения этого создаются резервные копии программ и документов. А большинство современных средств информационных технологий предусматривают автоматическое сохранение информационного продукта в ходе его разработки.

* Способы антивирусной защиты составляют технические и программные средства по защите информации от вирусов.
* Вирус — это программа содержащая, вредоносный код, поэтому основным средством от их защиты является антивирусное ПО — приложение, обеспечивающее отслеживание и уничтожение вирусов.
* Как и вирусы, антивирусы постоянно развиваются. Также постоянно расширяю ция антивирусного ПО.

Основная специфика вируса - это его **саморепликация**, за счёт которой он становится способным **внедрять свой код** в другие ПО, тем самым их заражая.

*Троян

Основная специфика трояна - это **обманывать** жертв, за счёт применения **оболочки невредоносного ПО**. Вследствие этого, чистая форма трояна выражается лишь его оболочкой, ни более ни менее.

В сравнении с вирусом (а также со множеством других ВПО), троян не имеет как таковых алгоритмов исполнения, потому как таковой является лишь оболочкой, формой без содержания. Сам по себе он бессмысленнен, как и вирус, не исполняющий конкретную логику, но лишь за счёт подобных сведений к чистым функциям мы далее сможем более качественно рассматривать композиции разнородных ПО.

* Червь

Основная специфика червя - это его **самореплицирование**, за счёт которой он становится способным **дублировать себя** как в пределах одной системы, создавая многочисленные копии в каталогах, так и **перемещаясь по системам**, создавая в каждой отдельной свою копию.

В отличие от вируса, обладающего точно также механизмом самореплицирования, червь не внедряется в уже существующее ПО, а создаёт свою копию как отдельный файл.

* Шифровальщик

Основная специфика шифровальщика - это **шифрование файлов** на системе жертвы, таким образом, чтобы жертва **не могла восстановить** всё ранее зашифрованное. В таком случае, жертва просто теряет все файлы, которые она когда-либо сохраняла.

Часто шифровальщик также именуют и **вымогателем**, что в определённой степени оправданно, т.к. таковой часто и самолично предлагает способ расшифровать все ранее зашифрованные им же файлы за выкуп в денежном эквиваленте.

В отличие от ранее рассмотренных вирусов, троянов и червей, не располагающих как таковой деструктивной логикой в своём исполнении, - шифровальщики напротив представляют в качестве чистой логики неприкрытый процесс разрушения.

* Локер

Основная специфика локера - это **блокирование действий** жертвы при работе в системе. В таком случае жертва либо не может подвигать мышкой, либо не может просматривать файлы или вовсе может не иметь доступ к файловой системе.

Локер также иногда именуют **вымогателем**, когда таковой блокирует экран жертвы и выводит на экран поле ввода пароля разблокировки и реквизиты с необходимостью «выкупить» возможность далее пользоваться системой.

* Программа удалённого доступа

Программа удалённого доступа сама по себе **не является вредоносным ПО**, тем не менее, **может использоваться как таковое**. В представлении чистых функций программы удалённого доступа являют собой исключительно факт передачи данных от одной системы к другой, ни более ни менее. Сопутствующие действия (включая деструктуризирующие) могут рассматриваться как комбинация применений нескольких программ.

* Стиллер

Основная специфика стиллера - это **автоматическая кража** информации с системы жертвы. В отличие от вирусов, червей, троянов, программ удалённого доступа стиллер сводит чистую функцию к конкретному действию-результату, аналогично локерам и шифровальщикам.

* Спамер

Основная специфика спамера - это **создание, выдача или замена рекламных банеров** в браузерах, приложениях, сайтах, а также возможная **рассылка сообщений** по мессенджерам, социальным сетям и почте.

* Установщик

Основная специфика установщика - это **автоматическое скачивание и запуск программ**. Но в отличие от удалённого доступа, действия которого осуществляются ручным способом и **направлены от злоумышленника к жертве**, установщики действуют полностью автономно по конкретно заданному алгоритму, а их действия противоположны удалённому доступу и **направлены от жертвы к злоумышленнику**.

*Логическая бомба

Основная специфика логичкой бомбы - это **считывание условия** при котором будет происходить распаковка и/или запуск определённого ПО.
В отличие от множества других ВПО, логическая бомба не самодостаточна и можно сказать бесполезна, ровно, как и программа удалённого доступа, вирус, троян, червь, руткит, буткит без сопутствующей логики исполнения (вредоносной нагрузки).

*Очиститель

Основная специфика очистителя - это **безвозвратное удаление** всех возможных файлов на системе жертвы.
В отличие от множества шифровальщиков, дающих возможность расшифровать всю зашифрованную информацию за счёт перевода денег, очистители действуют более радикально.

*Инициализатор

Основная специфика инициализатора - это установка вредоносного ПО в процесс автоматического запуска операционной системой после своего старта.

* Все вышеописанные виды вредоносных ПО мы можем классифицировать по их чистым функциям.
* Так например, мы можем увидеть, что некоторые ВПО в качестве чистой функции располагают точно заданной конечной логикой своего исполнения, как например, шифровальщики, локеры, стиллеры, спамеры, ботнеты, очистители. Они могут существовать (чисто теоретически) в полном отрыве от всех других ВПО и исполнять свою полезную нагрузку. Таковые ВПО далее мы будем именовать **исполнителями**.
* Далее, мы также можем заметить ещё одну закономерность, объединяющую другие ВПО воедино, а именно сама специфика транспортирования. Трояны, черви, программы удалённого доступа и установщики представляют собой методы передачи ВПО от одной системы к другой. В отличие от исполнителей, чистая функция которых сводится к конечной логике, ради которой ВПО и создавалось, чистая функция вышеописанных программ сводится исключительно к способам передачи других ВПО, самих себя или всё вместе для увеличения масштаба распространения ВПО по множеству систем. Таковые ВПО далее мы будем именовать **распространителями**.
* В завершении, мы можем отнести все оставшиеся ВПО, а именно - вирусы, руткиты, буткиты, логические бомбы, инициализаторы к **помощникам**, чистой функцией которых становится поддержание других ВПО, придание им свойств отказоустойчивости, живучести и скрытности. В отличие от распространителей, передающих ВПО от одной системы к другой, помощники живут исключительно в одной системе. В отличие от исполнителей, выполняющих базовое предназначение, помощники исполняют второстепенную роль в сопутствующей поддержке других ВПО для успешного осуществления основного предназначения.

Исполнители	Распространители	Помощники
Шифровальщик	Троян	Вирус
Локер	Червь	Логическая бомба
Стиллер	Программа удалённого доступа	Руткит
Спамер	Установщик	Буткит
Ботнет		Инициализатор
Очиститель		

Использование надежного пароля является одним из наиболее важных факторов защиты компьютера от злоумышленников и других нежелательных пользователей.

Пароль — это условное слово или набор знаков, предназначенный для подтверждения личности или полномочий.

Пароль, несущий в себе высокую степень защиты, должен отвечать следующим требованиям:

длина не менее 6—8 символов;

использование цифр;

использование букв разных регистров;

использование букв разных алфавитов;

использование специальных символов.

Плохие пароли	Хорошие пароли
123456789	D)dzq4Smo@
password	4j~8GvG{qB
qwerty	Re18ZEVH1#
master	Hx4@5g8DoJ
login1	%FfZMv4vDu
1a2s3d4f5g	pWjtbQ$g6B

5. КИБЕРБЕЗОПАСНОСТЬ: КАК ЗАЩИТИТЬ ЛИЧНЫЕ ДАННЫЕ В СЕТИ

Немного статистики

* 22% сталкивались с кражей аккаунтов в социальных сетях или играх
* 15% теряли данные из-за компьютерного вируса
* 14% отметили, что им писали странные сообщения взрослые
* 10% сталкивались с мошенничеством с использованием фальшивых сайтов и писем

Защита информации

* **Пароли**

* **Изучение политики конфиденциальности**

Прежде чем установить приложение или браузерное расширение, воспользоваться онлайн-сервисом или зарегистрироваться в социальной сети, обязательно изучите политику конфиденциальности. Убедитесь, что приложение или сайт не получает права распоряжаться вашими личными данными — фотографиями, электронным адресом или номером телефона.

* **Разрешения для приложений**

Многие приложения запрашивают данные об электронной почте или доступ к камере, фотогалерее и микрофону. Не выдавайте разрешений автоматически, следите за тем, какую информацию запрашивает приложение. В некоторых случаях разумнее вообще отказаться от его использования, чтобы не передавать личные данные о себе неизвестным лицам.

* **Настройки браузера**

Не разрешайте браузеру автоматически запоминать пароли к личным сайтам и страницам, а лучше отключите эту опцию в настройках. Автосохранение паролей увеличивает риск взлома личных страниц.

* **Чистка cookies**

Файлы cookies — это временные файлы интернета, которые хранятся на вашем устройстве и содержат информацию о сайтах, которые вы посещаете. С их помощью также можно отслеживать вашу активность в интернете, ваши интересы и предпочтения.

* **Блокировка рекламы**

Специальные программы, блокирующие рекламу, одновременно отслеживают попытки посторонних программ получить информацию с вашего компьютера, поэтому

* Защищённое соединение

Сайты, содержащие конфиденциальную информацию пользователей (сайты банков, государственных учреждений, онлайн-магазинов), обычно используют специальные протоколы передачи данных.

При защищённом соединении данные шифруются с помощью технологии SSL, после чего информация становится недоступна для третьих лиц.

Если в адресной строке браузера перед адресом сайта **https://** вы видите зелёный замочек, значит, сайт использует защищённое соединение. Обращайте на это внимание, когда вводите на сайте логин, пароль, номер банковской карты или другие личные данные.

* Домашний Wi-Fi

Пользоваться открытыми сетями Wi-Fi в кафе или торговом центре небезопасно, злоумышленники могут использовать их для взлома компьютера или смартфона и кражи паролей. В общественном месте не заходите на сайты, которые требуют ввода паролей и личных данных, делайте это по мобильной сети или через домашний Wi-Fi.

Безопасное общение

* **Кибербуллинг**

Травля по интернету — это угрозы и оскорбления от агрессивно настроенных пользователей в адрес другого пользователя. Заниматься кибербуллингом в ваш адрес может один или несколько человек. Чтобы не пострадать от подобной травли, соблюдайте несколько правил:

* Не отвечайте на агрессивные сообщения — обидчики только и ждут вашей ответной реакции.
* Занесите пользователей в чёрный список.
* Сообщите о происходящем технической поддержке социальной сети. Вам помогут заблокировать пользователя или же написать на него жалобу.
* Делайте скриншоты переписки, содержащей оскорбления и угрозы, чтобы в случае необходимости использовать её как доказательство травли против вас. На скриншотах должен быть виден текст сообщения и имя отправителя. Не полагайтесь на хранение переписки — в некоторых соцсетях и мессенджерах можно удалить отправленные сообщения.
* Сообщите о происходящем взрослым. Если угрозы направлены на жизнь и здоровье, то имеет смысл обратиться в правоохранительные органы.

* **Онлайн-груминг**

Грумингом называют различные виды мошенничества в сети, когда преступники обманом втираются в доверие к пользователям и получают от них личные данные или деньги за

Что нужно запомнить

🙂 Внимательно отнеситесь к созданию и хранению паролей.

🤐 Изучите политику конфиденциальности сайтов и приложений, запретите вашему браузеру автоматически сохранять пароли, регулярно удаляйте cookies.

🤑 Пользуйтесь блокировщиками рекламы.

🙄 Оставляйте личные данные только на сайтах с защищённым соединением. Не пользуйтесь общественными сетями Wi-Fi для передачи конфиденциальной информации.

😬 Если вы столкнулись с травлей в сети, блокируйте пользователя, который отправляет вам агрессивные сообщения. Обратитесь в службу поддержки сайта или социальной сети, сообщите родителям. Не вступайте в дискуссии с агрессивно настроенными пользователями.

🤯 Чтобы не стать жертвой интернет-мошенников, перепроверяйте всю информацию, полученную по электронной почте или в сообщениях социальных сетей и мессенджеров, не сообщайте незнакомым людям и не публикуйте в открытом доступе личные данные.

* **РЭШ HTTPS://RESH.EDU.RU/SUBJECT/LESSON/6472/TRAIN/166788/**

* **ИНФОРМАТИКА. 11 КЛАСС**

* **Урок 18. Информационное право и информационная безопасность**

ПОЙТИ ТРЕНИРОВОЧНЫЙ ТЕСТ!!!