**IT-Колледж “Сириус”**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**ДОКЛАД**

по дисциплине “Введение в специальность”

на тему “Кибербезопасность”

Выполнил:  
Студент группы

1.9.7.1  
Шеина Елизавета Сергеевна

Принял:

Старший преподаватель  
Тенигин Альберт Андреевич

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IT-Колледж “Сириус”  
2022

**Содержание**

Введение………...…………………………………………………………………3Что такое кибербезопасность?…………………………...……………………....4Меры обеспечения безопасности компьютерных систем…………………….6 Парольные системы идентификации и аутентификации пользователей………6 Вредоносное ПО….....……………………..……...………………………………8 Как защититься от атак: полезные советы по кибербезопасности…………….14 Заключение……………………………………………………………………….15 Список используемой литературы………………………………………….…..16

**Введение**

Информация является одним из фундаментальных понятий современности и относится к разряду тех, которые имеют очень широкое употребление.

Информационные взаимодействия – это основа существования как живой, так и неживой природы. Без информационных процессов немыслима и социальная жизнь. Информационные технологии представляют собой основу современной и особенно зарождающейся цивилизации – информационного общества.

Термин «информация» происходит от латинского слова «informatio», что означает сведения, разъяснения, изложение. Обычно под информацией понимаются знания, сведения, данные, сообщения и сигналы, с которыми мы имеем дело в повседневной жизни и проявление которых мы наблюдаем в природе и обществе. Определение информации, которое содержится в энциклопедическом словаре, говорит о том, что «информация – это общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом, 9 обмен сигналами в животном и растительном мире; передачу признаков от клетки к клетке, от организма к организму».

Правовое определение «информации» ввёл Федеральный закон (ФЗ) «Об информации, информатизации и защите информации». В соответствии с ним «информация – это сведения о лицах, предметах, фактах, событиях, процессах независимо от формы их представления». Позже этот ФЗ утратил силу и его преемником стал ФЗ «Об информации, информационных технологиях и о защите информации».

В новом законе интересующее нас определение было немного изменено: «информация – сведения (сообщения, данные) независимо от формы их представления». В научной литературе можно встретить десятки попыток дать определение «информации». Многие специалисты признают, что даже достаточно полного, не говоря уж о всеобъемлющем, определения информации дать невозможно, что в каждой научно-прикладной ситуации её определение имеет «своё лицо» и выполняет свои функции.

Данные – фиксируемые в виде определенных сигналов воспринимаемые факты окружающего мира.

Данные несут в себе сведения о событиях, произошедших в материальном мире, и являются регистрацией сигналов, возникших в результате этих событий. Однако данные не тождественны информации. Станут ли данные информацией – зависит от того, известен ли метод преобразования данных в известные понятия.

# **Что такое кибербезопасность?**

Кибербезопасность (иногда называемая компьютерной безопасностью) - это набор методов и практик защиты от вредоносных атак на компьютеры, серверы, мобильные устройства, электронные системы, сети и данные. Кибербезопасность находит применение в самых разных областях, от сферы бизнеса до мобильных технологий. В этом направлении существует несколько основных категорий.

* **Безопасность сетей**
* **Безопасность приложений**
* **Безопасность информации**
* **Операционная безопасность**
* **Аварийное восстановление и непрерывность бизнеса**

## Масштаб распространения киберугроз:

Год за годом в мире становится все больше угроз и происходит все больше утечек данных. Статистика шокирует: согласно отчету [RiskBased Security](https://www.riskbasedsecurity.com/2019/11/12/number-of-records-exposed-up-112/), только за первые девять месяцев 2019 года было зафиксировано 7,9 миллиардов случаев утечки данных. Эти цифры превышают показатели за тот же период 2018 года более чем в два раза (на 112 %).

Чаще всего утечке данных подвергаются медицинские и государственные учреждения или организации из сферы розничной торговли. В большинстве случаев причина – действия преступников. Некоторые организации привлекают злоумышленников по понятной причине – у них можно украсть финансовые и медицинские данные. Однако мишенью может стать любая компания, ведь преступники могут охотиться за данными клиентов, шпионить или готовить атаку на одного из клиентов.

Компания International Data Corporation прогнозирует, что если количество киберугроз будет расти и дальше, то объем расходов на решения в области кибербезопасности к 2022 году достигнет 133,7 миллиардов долларов. Правительства разных стран борются с преступниками, помогая организациям внедрять эффективные методы кибербезопасности.

Понятие информационной безопасности

В повседневной жизни часто информационная безопасность (ИБ) понимается лишь как необходимость борьбы с утечкой секретной и распространением ложной и враждебной информации. Однако, это понимание очень узкое. Существует много разных определений информационной безопасности, в которых высвечиваются отдельные её свойства. В утратившем силу ФЗ «Об информации, информатизации и защите информации» под информационной безопасностью понималось состояние защищённости информационной среды общества, обеспечивающее её формирование и развитие в интересах граждан, организаций и государства.

Информационная безопасность – это

Защита информации

Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

**Меры обеспечения безопасности компьютерных систем.**

По способам осуществления все меры обеспечения безопасности компьютерных систем подразделяют на:

* правовые (законодательные);
* морально-этические;
* организационно-административные;
* физические;
* аппаратно-программные.

Остановимся на аппаратно-программных мерах защиты. К ним относятся различные электронные устройства и специальные программы, которые реализуют самостоятельно или в комплексе с другими средствами следующие способы защиты:

* идентификацию и аутентификацию субъектов АСОИ;
* разграничение доступа к ресурсам АСОИ; – контроль целостности данных; – обеспечение конфиденциальности данных;
* аудит событий, происходящих в АСОИ;
* резервирование ресурсов и компонентов АСОИ.

**Парольные системы идентификации и аутентификации пользователей**

Совокупность идентификатора и пароля пользователя — основные составляющие его учетной записи. База данных пользователей парольной системы содержит учетные записи всех пользователей КС, при этом сами пароли шифруются администратором сети, обычно с использованием хеш-функций.

Парольные системы являются зачастую «передним краем обороны» всей системы безопасности. Отдельные ее элементы могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику (в том числе и база данных учетных записей пользователей). В связи с этим парольные системы становятся одним из наиболее привлекательных для злоумышленника объектов атаки.

Основными типами угроз безопасности парольных систем являются следующие.

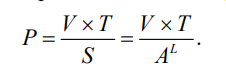
* Перебор паролей в интерактивном режиме.
* Подсмотр пароля.
* Преднамеренная передача пароля его владельцем другому лицу.
* Кража базы данных учетных записей с дальнейшим ее анализом, подбором пароля.
* Перехват вводимого пароля путем внедрения в КС программных закладок (клавиатурных шпионов); перехват пароля, передаваемого по сети.
* Социальная инженерия.

Для уменьшения деструктивного влияния человеческого фактора необходимо реализовать ряд требований к выбору и использованию паролей:

* Задание минимальной длины пароля для затруднения подбора пароля злоумышленником «в лоб» и подсмотра
* Использование в пароле различных групп символов для усложнения подбора злоумышленником пароля.
* Проверка и отбраковка пароля по словарю для затруднения подбора пароля злоумышленником с использованием словарей.
* Установление максимального срока действия пароля для затруднения подбора пароля злоумышленником, в том числе и в режиме off-line при взломе предварительно похищенной базы данных учетных записей пользователей.
* Применение эвристического алгоритма, бракующего «плохие» пароли для усложнения подбора пароля злоумышленником «по словарю» или с использованием эвристического алгоритма.Ограничение числа попыток ввода пароля для предотвращения интерактивного подбора пароля злоумышленником.
* Использование задержки при вводе неправильного пароля для предотвращения интерактивного подбора пароля злоумышленником.
* Поддержка режима принудительной смены пароля пользователя для эффективности реализации требования, ограничивающего максимальный срок действия пароля.
* Запрет на выбор пароля самим пользователем и автоматическая генерация паролей для затруднения использования злоумышленником эвристического алгоритма подбора паролей.

Количественная оценка стойкости парольных систем может быть выполнена с помощью рассматриваемого ниже подхода. Пусть A — мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля). Например, если при составлении пароля могут быть использованы только малые английские буквы, то A = 26. L — длина пароля.

S = AL — число всевозможных паролей длины L, которые можно составить из символов алфавита A. S также называют пространством атаки. V — скорость перебора паролей злоумышленником. T — максимальный срок действия пароля. Тогда вероятность P подбора пароля злоумышленником в течение срока его действия Т определяется по следующей формуле:



### **Вредоносное ПО**

Название говорит само за себя. Программное обеспечение, которое наносит вред, – самый распространенный инструмент киберпреступников. Они создают его сами, чтобы с его помощью повредить компьютер пользователя и данные на нем или вывести его из строя. Вредоносное ПО часто распространяется под видом безобидных файлов или почтовых вложений. Киберпреступники используют его, чтобы заработать или провести атаку по политическим мотивам.

Вредоносное ПО может быть самым разным, вот некоторые распространенные виды:

* **Вирусы –** программы, которые заражают файлы вредоносным кодом. Чтобы распространяться внутри системы компьютера, они копируют сами себя.
* **Троянцы–** вредоносы, которые прячутся под маской легального ПО. Киберпреступники обманом вынуждают пользователей загрузить троянца на свой компьютер, а потом собирают данные или повреждают их.
* **Шпионское ПО –** программы, которые втайне следят за действиями пользователя и собирают информацию (к примеру, данные кредитных карт). Затем киберпреступники могут использовать ее в своих целях.
* **Программы-вымогатели** шифруют файлы и данные. Затем преступники требуют выкуп за восстановление, утверждая, что иначе пользователь потеряет данные.
* **Рекламное ПО –** программы рекламного характера, с помощью которых может распространяться вредоносное ПО.
* **Ботнеты –** сети компьютеров, зараженных вредоносным ПО, которые киберпреступники используют в своих целях.

### **SQL-инъекция**

Этот вид кибератак используется для кражи информации из баз данных. Киберпреступники используют уязвимости в приложениях, управляемых данными, чтобы распространить вредоносный код на языке управления базами данных (SQL).

## **Типы SQLi**

Существует 5 основных типов SQL инъекций:

* Классическая (In-Band или Union-based). Самая опасная и редко встречающаяся сегодня атака. Позволяет сразу получать любые данные из базы.
* Error-based. Позволяет получать информацию о базе, таблицах и данных на основе выводимого текста ошибки СУБД.
* Boolean-based. Вместо получения всех данных, атакующий может поштучно их перебирать, ориентируясь на простой ответ типа true/false.
* Time-based. Похожа на предыдущую атаку принципом перебора, манипулируя временем отклика базы.
* Out-of-Band. Очень редкие и специфические типы атак, основанные на индивидуальных особенностях баз данных.

## **Уязвимые точки**

Уязвимые точки для атаки находятся в местах, где формируется запрос к базе: форма аутентификации, поисковая строка, каталог, REST-запросы и непосредственно URL.

9

**Защита от SQL**

Для каждого сервера и фреймворка есть свои тонкости и лучшие практики, но суть всегда одинакова.

Нельзя вставлять данные в запрос напрямую. Всегда обрабатывайте ввод отдельно и формируйте запрос исключительно из безопасных значений.

Создавайте белые списки: их значительно труднее обойти, чем черные. Все названия таблиц, полей и баз должны быть заданы конкретными значениями в вашей программе. Это касается и операторов.

Естественно, не забывайте про ограничение прав доступа к базе.

Тем не менее, кибербезопасность – это тот случай, когда понимание принципов нападения – лучший способ защиты.

**Фишинг** – атаки, цель которых – обманом заполучить конфиденциальную информацию пользователя (например, данные банковских карт или пароли). Часто в ходе таких атак преступники отправляют жертвам электронные письма, представляясь официальной организацией.

Фишинг – вид интернет-мошенничества для получения доступа к личным данным пользователя: логинам и паролям, номерам карт, банковским счетам. Как и рыбаки, использующие множество способов ловли рыбы, мошенники применяют разные методы, чтобы поймать жертву «на крючок». Став жертвой фишинга, можно лишиться денег или доступа к своим аккаунтам, пустить хакера в корпоративную сеть работодателя.

Наиболее распространенная тактика фишинга выглядит следующим образом. Пользователь получает электронное письмо, которое внешне может быть очень похоже на настоящее сообщение от популярных организаций: банков, компаний, органов власти или госуслуг. Если пользователь «клюет на наживку» и переходит по ссылке из письма, он попадает на поддельный сайт, внешне неотличимый от настоящего. Введенные на этом сайте данные отправляются напрямую к злоумышленникам, которые затем используют их для кражи персональной информации или денег с банковских счетов. Фишинговыми бывают не только письма, приходящие на электронную почту. Это могут быть сообщения в мессенджерах, социальных сетях и смс.

### Поддельные приложения

В своих схемах мошенники используют приложения для смартфонов, планшетов и компьютеров. Эти программы содержат вирусы, крадут логины и пароли от онлайн-банка, а также перехватывают смс с кодами. Чаще всего подделывают приложения мобильных банков – если ввести логин и пароль в такой программе, хакеры получат доступ к вашим счетам в настоящем приложении.

Скачивайте программы из официальных магазинов приложений, обращая внимание на количество скачиваний, рейтинг и отзывы. Если программа совсем новая и ее пока мало кто установил, лучше не рисковать. Если необходимо установить или обновить приложения банков, попавших под санкции, скачивайте их с официальных сайтов организаций.

### **Атаки Man-in-the-Middle** («человек посередине»)

Это атака, в ходе которой киберпреступник перехватывает данные во время их передачи – он как бы становится промежуточным звеном в цепи, и жертвы об этом даже не подозревают. Вы можете подвергнуться такой атаке, если, например, подключитесь к незащищенной сети Wi-Fi.

Концепция MITM-нападения (**Man-in-the-Middle**) на удивление проста, и она не ограничивается безопасностью компьютера или онлайн-ресурса. В самом простом случае злоумышленнику надо всего лишь поставить себя в цепь между двумя общающимися сторонами, чтобы перехватывать их сообщения друг другу. При этом злоумышленник всегда должен выдавать себя за каждую из противоположных сторон. Например, в реальной жизни можно создать поддельный счет и положить его в почтовый ящик жертвы. После чего перехватить его на почте, когда жертва попытается счет оплатить. В онлайне все намного сложнее, но суть та же. Злоумышленник ставит себя между целью и ресурсом, требуемым цели. При этом наличие атакующего всегда должно оставаться незаметным для обеих сторон. В этом залог успеха атаки.

## **Варианты MITM-атаки**

Больше всего распространены MITM-атаки, когда злоумышленник использует Wi-Fi-маршрутизатор в качестве инструмента перехвата сообщений. В данном случае создается подмена используемого роутера и подмена самой сети. Либо используются ошибки в настройке и защите сети, позволяющие вполне легально перехватывать сессии. В первом сценарии злоумышленник настраивает в своем ноутбуке точку беспроводного доступа, давая ей то же имя, что и используемое в общественном месте с доступным Wi-Fi. Когда пользователи подключаются к этой псевдосети, то при попытке совершить какое-либо действие с коммерческими сайтами, банковскими или прочими финансовыми ресурсами, их информация перехватывается, после чего злоумышленник уже может пользоваться ей по своему усмотрению.

Второй вариант сценария предполагает, что [злоумышленник находит уязвимости в настройке или шифровании в легальной сети](https://threatpost.com/en_us/blogs/new-attack-breaks-confidentiality-model-ssl-allows-theft-encrypted-cookies-091911), после чего использует этот недостаток для слежения за жертвами. Это более сложный путь, но он может быть не менее эффективным, если атакующий имеет постоянный доступ к интересующему его роутеру в течение длительного времени. Это дает ему возможность незаметно «прослушивать» интересующую сессию и, пока жертва считает, что она в безопасности, собирать большое количество нужной информации.

В последнее время встречается и вариант MITM-атаки «Человек-в-браузере». В этом случае злоумышленник использует один из нескольких возможных методов для того, чтобы занести вредоносный код, работающий внутри браузера, на компьютер жертвы. Это ПО потом незаметно записывает все данные, передаваемые между браузером и различными сайтами, после чего отсылает полученные сведения злоумышленнику. Такой вариант становится все более распространенным, так как он может применяться к большой группе пользователей-жертв, а также не требует, чтобы злоумышленник находился поблизости.

## **Защита**

Есть несколько эффективных средств защиты от MITM-атак, но почти все они используются либо в самом маршрутизаторе, либо на серверах, к которым обращается потенциальная жертва. При этом самой жертве невдомек, на настоящем она сервере либо это подделка, подставленная злоумышленником. Одним из способов защиты от такой атаки является использование стойкого шифрования между клиентом и сервером. В таком случае сервер может идентифицировать себя посредством предоставления цифрового сертификата, после чего между пользователем и сервером устанавливается шифрованный канал для обмена конфиденциальными данными. Но в этом случае возникает зависимость от самого сервера и выбора им метода шифрования.

Другим вариантом защиты от некоторых видов MITM-атак является полный отказ от использования открытых Wi-Fi-сетей для работы с личными данными. Хорошую защиту дают некоторые плагины для браузеров. Например, [HTTPS Everywhere](https://www.eff.org/https-everywhere) или [ForceTLS](http://forcetls.sidstamm.com/), которые самостоятельно устанавливают защищенное соединение всякий раз, когда эта опция доступна на стороне сервера. Но, как бы то ни было, все способы защиты имеют определенные ограничения. Кстати, не стоит забывать и об уже проведенных с целью демонстрации возможностей атаках, таких как [SSLStrip](https://threatpost.com/en_us/blogs/how-render-ssl-useless-081810) или SSLSniff, которые легко сведут на нет безопасность SSL-соединения.

### **DoS-атаки** (атаки типа «отказ в обслуживании»)

Киберпреступники создают избыточную нагрузку на сет и и серверы объекта атаки, из-за чего система прекращает нормально работать и ею становится невозможно пользоваться. Так злоумышленники, например, могут повредить важные компоненты инфраструктуры и саботировать деятельность организации.

Сетевые ресурсы, такие как веб-серверы, имеют ограничения по количеству запросов, которые они могут обслуживать одновременно. Помимо допустимой нагрузки на сервер существуют также ограничения пропускной способности канала, который соединяет сервер с Интернетом.

Когда количество запросов превышает производительность любого компонента инфраструктуры, может произойти полное прекращение работы веб-ресурса – «отказ в обслуживании» или DoS (Dental-of-service).

Также, в зависимости от целей злоумышленника, результатом работы могут быть:

* Существенное замедление время ответа на запросы;
* Отказ в обслуживании части пользовательских запросов;
* Прикрытие другой зловредной активности на web-ресурсе жертвы;
* **Топливо для DDoS-атак**
* Для отправки очень большого количества запросов на ресурс жертвы киберпреступник часто создает сеть из зараженных «зомби-компьютеров» и любых других устройств, подключённых к сети.
* Поскольку преступник контролирует действия каждого зараженного компьютера в зомби – сети , атака может быть слишком мощной для веб-ресурса жертвы.
* Масштабы зомби-сетей впечатляющие. Например, вовремя не обновлённая уязвимость домашних роутеров одно известного вендора позволила заразить и управлять сетью из более 500.000 устройств по всему миру.

**Меры противодействия DDoS-угрозам**

В настоящее время такая преступная деятельность получила колоссальное распространение. Количество и мощность DDoS-атак растет. Однако количество **успешных** DDoS-атак уменьшается.

В подавляющем большинстве случаев для защиты от DDoS-атак задействуются специализованные компании, что гораздо дешевле самостоятельно организации защиты внутри компании и уж тем более, стоимости последствий успешной DDoS-атаки.

## **Как защититься от атак: полезные советы по кибербезопасности**

* **Обновите программное обеспечение и операционную систему.** Используя новое ПО, вы получаете свежие исправления безопасности.

#### **Используйте антивирусные программы.** Защитные решения, такие как Kaspersky Total Security, Dr.Web, ESET NOD32, Защитник Windows

помогут выявить и устранить угрозы. Для максимальной безопасности регулярно обновляйте программное обеспечение.

* **Используйте надежные пароли.** Не применяйте комбинации, которые легко подобрать или угадать.
* **Не открывайте почтовые вложения от неизвестных отправителей –** они могут быть заражены вредоносным ПО.
* **Не переходите по ссылкам, полученным по почте от неизвестных отправителей или неизвестных веб-сайтов –** это один из стандартных путей распространения вредоносного ПО.
* **Избегайте незащищенных сетей Wi-Fi в общественных местах – в** них вы уязвимы для атак Man-in-the-Middle.

**Вывод**

Подведем итоги

Следуйте простым правилам, чтобы обеспечить свою безопасность и не стать жертвой интернет-мошенников.

Внимательно проверяйте адрес отправителя.

Ищите информацию об акциях или выплатах на официальных сайтах компаний и ведомств.

Изменяйте учетные данные не по ссылке из письма, а самостоятельно зайдя на сайт.

Не переходите по подозрительным ссылкам.

Не открывайте присланные файлы, если не уверены в отправителе.

Не устанавливайте приложения из сомнительных источников.

**Список используемой литературы**

1. О. В. ПРОХОРОВА ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ УЧЕБНИК Издание второе, стереотипное
2. В. В. Гафнер ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ Учебное пособие Часть 1
3. <https://proglib.io/p/vzlamyvaem-sayty-shpargalka-po-sql-inekciyam-2019-12-21>

# [Ю. Родичев "Нормативная база и стандарты в области информационной безопасности" (2017)](https://www.ozon.ru/context/detail/id/137707095/)

* комплекс орг
* анизационно-технических мероприятий, обеспечивающих целостность данных и конфиденциальность информации в сочетании с её доступностью для всех авторизовпоказатель, отражающий статус защищенности инфорсостояние защищённости информационной сресостояние, обеспечивающее защищенность информационных ресурсов и каналов, а также доступа к источникам информации.