**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?…………………………...……………………....3Меры обеспечения безопасности компьютерных систем…………………….5 Парольные системы идентификации и аутентификации пользователей...……5 Вредоносное ПО….....……………………..……...………………………………6 SQL-инъекция……………………………………………………………………..7 Атаки Man-in-the-Middle………………………………………………………….9 DoS-атаки………………………………...……………………………………………………11 Как защититься от атак: полезные советы по кибербезопасности..………….11 Заключение……………………………………………………………………….12 Список используемой литературы………………………………………….…..13

Введение

Информация считается одним из базовых мнений нашего времени и относится к уровню тех, которые имеют довольно обширное использование.  
Термин «информация» случается от латинского текста «informatio», собственно что значит сведения, объяснения, изложение. Как правило под информацией понимаются познания, сведения, данные, сообщения и сигналы, с которыми мы имеем дело в будничной жизни и проявление коих мы присматриваем в природе и обществе. Определение инфы, которое находится в энциклопедическом словаре, беседует о том, собственно что «информация – это общенаучное понятие.  
Правовое определение «информации» ввёл Федеральный закон (ФЗ) «Об инфы, информатизации и обороне информации». В согласовании с ним «информация – это сведения о лицах, предметах, прецедентах, мероприятиях, процессах автономно от формы их представления». Позднее данный ФЗ потерял мощь и его преемником стал ФЗ «Об инфы, информационных разработках и о обороне информации».  
Данные – закрепляемые в облике конкретных сигналов воспринимаемые прецеденты находящегося вокруг мира. Данные несут в для себя сведения о мероприятиях, произошедших в вещественном мире, и считаются регистрацией сигналов, образовавшихся в итоге данных мероприятий.

# Что такое кибербезопасность?

Кибербезопасность (иногда именуемая компьютерной безопасностью) - это комплект способов и практик обороны от вредных атак на компы, серверы, мобильные прибора, электрические системы, сети и данные. Кибербезопасность находит использование в самых различных областях, от сферы бизнеса до мобильных технологий. В данном направленности есть некоторое количество ведущих категорий.

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

## Масштаб распространения киберугроз:

## Год за годом в мире делается все более опасностей и случается все более утечек данных. Статистика шокирует: сообразно докладу RiskBased Security, лишь только за 1-ые 9 месяцев 2019 года было закреплено 7,9 млрд случаев утечки данных. Эти цифры превосходят характеристики за что же этап 2018 года больше чем в 2 раза (на 112 %). Почаще всего утечке данных подвергаются мед и муниципальные учреждения или же организации из сферы розничной торговли. В большинстве случаев первопричина – воздействия преступников. Кое-какие организации влекут злодеев по понятной основанию – у их возможно похитить денежные и мед данные. Впрочем мишенью имеет возможность замерзнуть каждая фирма, так как злоумышленники имеют все шансы охотиться за данными покупателей, шпионить или же стряпать атаку на 1-го из покупателей. Фирма International Data Corporation предсказывает, собственно что в случае если численность киберугроз станет вырастать и далее, то размер затрат на заключения в области кибербезопасности к 2022 году добьется 133,7 млрд $. Правительства различных государств сражаются с правонарушителями, помогая организациям вводить действенные способы кибербезопасности. Информационная защищенность – это Оборона инфы Работа по предотвращению утечки защищаемой инфы, несанкционированных и ненамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение сего состояния.

Меры обеспечивания защищенности компьютерных систем.  
  
По методикам воплощения все меры обеспечивания защищенности компьютерных систем подразделяют на:

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

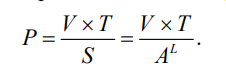
Парольные системы идентификации и аутентификации пользователей.

Совокупность личного номера и пароля юзера — главные элементы его учетной записи. Основа данных юзеров парольной системы имеет учетные записи всех юзеров КС, при данном сами пароли шифруются админом сети, как правило с внедрением хеш-функций.  
Парольные системы считаются нередко «передним краем обороны» всей системы защищенности. Отдельные ее составляющие имеют все шансы быть находятся в пространствах, раскрытых для доступа вероятному злодею (в что количестве и основа данных учетных записей пользователей). В связи с данным парольные системы делаются одним из более красивых для злодея объектов атаки.

Ведущими типами опасностей защищенности парольных систем считаются надлежащие.

•Перебор паролей в интерактивном режиме.  
•Подсмотр пароля.  
•Преднамеренная предоставление пароля его обладателем другому лицу.  
• Кража базы данных учетных записей с последующим ее анализом, подбором пароля.  
• Перехват вводимого пароля методом внедрения в КС программных закладок (клавиатурных шпионов); перехват пароля, передаваемого по сети.  
• Социальная инженерия.

Количественная оценка стойкости парольных систем имеет возможность быть исполнена с поддержкой рассматриваемого ниже расклада. Пусть A — мощность алфавита паролей (количество знаков, которые имеют все шансы быть применены при составлении пароля). К примеру, в случае если при составлении пароля имеют все шансы быть применены лишь только мелкие английские буковки, то A = 26. L — длина пароля.  
S = AL — количество различных паролей длины L, которые возможно составить из знаков алфавита A. S еще именуют местом атаки. V — скорость перебора паролей злоумышленником. T — наибольший срок воздействия пароля. За это время возможность P подбора пароля злоумышленником в направление срока его воздействия Т ориентируется по надлежащей формуле:



### Вредоносное ПО

Название говорит само за себя. Программное обеспечиние, которое наносит урон, – самый известный инструмент киберпреступников. Они делают его сами, дабы с его поддержкой разрушить компьютер юзера и данные на нем или же исключить его из строя. Вредное ПО нередко распространяется под обликом безопасных файлов или же почтовых инвестициям. Киберпреступники пользуют его, дабы заработать или же выполнить атаку по политическим мотивам.  
Вредное ПО имеет возможность быть наиболее различным, вот кое-какие известные облики:

Вирусы – программы, которые заражают файлы вредным кодом. Дабы распространяться изнутри системы комп, они копируют сами себя.  
• Троянцы– вредоносы, которые скрываются под маской законного ПО. Киберпреступники ложью заставляют юзеров нагрузить троянца на личный компьютер, а затем собирают данные или же повреждают их.  
•Шпионское ПО – программы, которые в секрете смотрят за деяниями юзера и собирают информацию (к примеру, данные кредитных карт). Вслед за тем киберпреступники имеют все шансы применить ее в собственных целях.  
•Программы-вымогатели шифруют файлы и данные. Вслед за тем злоумышленники настоятельно просят выкуп за восстановление, утверждая, собственно что по другому юзер потускнеет данные.  
•Рекламное ПО – программпы маркетингового нрава, с поддержкой коих имеет возможность распространяться вредное ПО.  
•Ботнеты – сети компов, инфицированных вредным ПО, которые киберпреступники пользуют в собственных целях.

### SQL-инъекция

Данный вид кибератак применяется для кражи инфы из баз данных. Киберпреступники пользуют уязвимости в приложениях, управляемых данными, дабы распространить вредный код на языке управления базами данных (SQL).

## Типы SQLi

Существует 5 основных типов SQL инъекций:

•Классическая (In-Band или же Union-based). Исключительно критическая и изредка встречающаяся сейчас нападение. Разрешает незамедлительно получать всевозможные данные из базы.  
• Error-based. Разрешает получать информацию о основе, таблицах и данных на базе выводимого слова промахи СУБД.  
•Boolean-based. Взамен получения всех данных, атакующий имеет возможность поштучно их перебирать, ориентируясь на незатейливый ответ на подобии true/false.  
•Time-based. Смахивает на предшествующую атаку принципом перебора, манипулируя периодом резонанса базы.  
•Out-of-Band. Довольно исключительные и своеобразные типы атак, базирующиеся на персональных особенностях баз данных.

Оборона от SQL

Для всякого сервера и фреймворка есть собственные тонкости и наилучшие практики, но сущность всякий раз схожа.  
Невозможно вставлять данные в запрос впрямую. Всякий раз обрабатывайте ввод порознь и формируйте запрос самая из неопасных значений.  
Делайте белоснежные перечни: их важно сложнее обогнуть, чем темные. Все наименования таблиц, полей и баз обязаны быть заданы определенными значениями в вашей программке. Это касается и операторов.  
Конечно, не запамятуйте на тему лимитирование прав доступа к основе.  
Что не наименее, кибербезопасность – это что случай, когда осознание основ нападения – наилучший метод обороны.

Фишинг – атаки, задача коих – ложью заполучить секретную информацию юзера (например, данные банковских карт или же пароли). Нередко в ходе этих атак злоумышленники отсылают потерпевшим электрические послания, представляясь официальной организацией.  
Фишинг – картина интернет-мошенничества для получения доступа к собственным сведениям юзера: логинам и паролям, номерам карт, банковским счетам. Став жертвой фишинга, возможно потерять средств или же доступа к собственным аккаунтам, пустить взломщика в корпоративную сеть работодателя.  
Более всераспространенная стратегия фишинга смотрится грядущим образом. Юзер получает электрическое послание, которое наружно имеет возможность быть довольно аналогично на реальное известие от известных организаций: банков, фирм, органов власти или же госуслуг. В случае если юзер «клюет на наживку» и перебегает по ссылке из послания, он попадает на фальшивый вебсайт, наружно неотличимый от истинного. Введенные на данном веб-сайте данные отправляются впрямую к злодеям, которые вслед за тем пользуют их для кражи индивидуальной инфы или же средств с банковских счетов. Фишинговыми случаются не лишь только послания, приходящие на электрическую почту. Это имеют все шансы быть сообщения в мессенджерах, общественных сетях и смс.  
Фальшивые приложения  
В собственных схемах аферисты пользуют приложения для телефонов, планшетов и компов. Эти программы содержат микробы, воруют логины и пароли от онлайн-банка, а еще перехватывают смс с кодами. Почаще всего подделывают приложения мобильных банков – в случае если установить логин и пароль в подобный программы, хакеры получат доступ к вашим счетам в подлинном приложении.  
  
  
Скачивайте программы из официальных магазинов приложений, обращая забота на численность скачек, рейтинг и отзывы. В случае если программка абсолютно свежая и ее пока же не достаточно кто установил, чем какого-либо другого не рисковать. В случае если нужно ввести или же подновить приложения банков, попавших под наказания, скачивайте их с официальных вебсайтов организаций.

Атаки Man-in-the-Middle

Это нападение, в ходе которой киберпреступник перехватывает данные во время их передачи – он как бы делается промежным звеном в цепи, и потерпевшие об данном в том числе и не подозревают. Вы сможете подвергнуться подобный нападению, в случае если, к примеру, подключитесь к беззащитной сети Wi-Fi.  
  
Концепция MITM-нападения (Man-in-the-Middle) на изумление ординарна, и она не ограничивается защищенностью компа или же онлайн-ресурса. В самом ординарном случае злодею надобно всего только поставить себя в цепь меж 2-мя контактирующими сторонами, дабы перехватывать их сообщения приятель приятелю. При данном преступник всякий раз обязан выдавать себя за любую из обратных сторон. К примеру, в реальной жизни возможно сделать фальшивый счет и положить его в почтовый ящик потерпевшие. Впоследствии чего перехватить его на почте, когда жертва захочет счет оплатить. В интернете все гораздо труднее, но сущность та же.  Преступник становит себя меж целью и ресурсом, требуемым цели. При данном присутствие атакующего всякий раз надлежит оставаться неприметным для обеих сторон. В данном задаток фурора атаки.

Варианты MITM-атаки

Более всего распространены MITM-атаки, когда преступник пользуется Wi-Fi-маршрутизатор в качестве инструмента перехвата извещений. В предоставленном случае формируется замена применяемого роутера и замена самой сети. Или применяются промахи в настройке и обороне сети, дозволяющие абсолютно законно перехватывать сессии. В первом сценарии преступник настраивает в собственном ноутбуке точку беспроводного доступа, давая ей то же имя, собственно что и применяемое в социальном пространстве с легкодоступным Wi-Fi. Когда юзеры включаются к данной псевдосети, то при попытке осуществить какое-либо воздействие с платными веб-сайтами, банковскими или же иными экономическими ресурсами, их информация перехватывается, впоследствии чего преступник уже имеет возможность воспользоваться ей по собственному усмотрению.  
2 вариант сценария подразумевает, собственно что преступник находит уязвимости в настройке или же шифровании в законной сети, впоследствии чего пользуется данный дефект для слежения за потерпевшими. Это больше трудный дорога, но он имеет возможность быть не наименее действенным, в случае если атакующий содержит неизменный доступ к интересующему его роутеру в направление долговременного времени. Это выделяет ему вероятность неприметно «прослушивать» интересующую сессию и, пока же жертва считает, собственно что она в защищенности, коллекционировать большущее численность необходимой инфы.  
В последнее время сталкивается и вариант MITM-атаки «Человек-в-браузере». В данном случае преступник пользуется раз из нескольких вероятных способов для такого, дабы занести вредный код, работающий изнутри браузера, на компьютер потерпевшие. Это ПО затем неприметно записывает все данные, передаваемые меж браузером и разными веб-сайтами, впоследствии чего отсылает приобретенные сведения злодею. Подобный вариант делается все больше всераспространенным, например как он имеет возможность использоваться к большущий группе пользователей-жертв, а еще не настятельно просит, дабы преступник располагался вблизи.

Оборона

Есть некоторое количество действенных средств обороны от MITM-атак, но практически все они применяются или в самом маршрутизаторе, или на серверах, к коим обращается вероятная жертва. При данном самой жертве невдомек, на подлинном она сервере или это фальшивка, подставленная злоумышленником. Одним из методик обороны от подобный атаки считается внедрение устойчивого шифрования меж покупателем и сервером. В этом случае сервер имеет возможность идентифицировать себя при помощи предоставления цифрового сертификата, впоследствии чего меж юзером и сервером уточняется шифрованный канал для обмена секретными данными. Но в данном случае появляется подневольность от самого сервера и выбора им способа шифрования.  
Иным вариантом обороны от кое-каких обликов MITM-атак считается абсолютный отказ от применения раскрытых Wi-Fi-сетей для работы с личностными данными. Неплохую защиту выделяют кое-какие плагины для браузеров. К примеру, HTTPS Everywhere или же ForceTLS, которые автономно ставят защищенное слияние любой раз, когда данная функция доступна на стороне сервера. Но, как бы то ни было, все методы обороны имеют конкретные лимитирования. Кстати, не стоит забывать и об уже проделанных с целью презентации вероятностей атаках, этих как SSLStrip или же SSLSniff, которые просто сведут на нет защищенность SSL-соединения.

### DoS-атаки

Киберпреступники делают сверхизбыточную нагрузку на сет и и серверы объекта атаки, по причине чего система прекращает неплохо трудиться и ею делается нельзя воспользоваться. Например злодеи, к примеру, имеют все шансы разрушить значимые составляющие инфраструктуры и саботировать работа организации.  
Сетевые ресурсы, эти как веб-серверы, имеют лимитирования по численности запросов, которые они имеют все шансы обслуживать в одно и тоже время. Кроме допустимой нагрузки на сервер есть еще лимитирования пропускной возможности канала, который объединяет сервер с Онлайном.  
Когда численность запросов выше производительность всякого компонента инфраструктуры, имеет возможность случится абсолютное остановка работы веб-ресурса – «отказ в обслуживании» или же DoS (Dental-of-service).  
Еще, в зависимости от целей злодея, итогом работы имеют все шансы быть:  
• Существенное замедление время ответа на запросы;  
• Отказ в обслуживании части пользовательских запросов;  
• Прикрытие иной зловредной энергичности на web-ресурсе потерпевшие

Меры противодействия DDoS-угрозам

В реальное время эта криминальная работа возымела колоссальное распространение. Численность и мощность DDoS-атак увеличивается. Впрочем численность удачных DDoS-атак миниатюризируется.  
В усмиряющем большинстве случаев для обороны от DDoS-атак задействуются специализованные фирмы, собственно что значительно выгоднее автономно организации обороны изнутри фирмы и уж что больше, цены результатов удачной DDoS-атаки.

## Как защититься от атак: полезные советы по кибербезопасности

 Обновите программное обеспечивание и операционную систему. Применяя свежее ПО, вы получаете бодрые поправки защищенности.  
Используйте антивирусные программки. Защитные заключения, эти как Kaspersky Total Security, Dr.Web, ESET NOD32, Адвокат Windows  
несомненно помогут обнаружить и убрать опасности. Для наибольшей защищенности периодически обновляйте программное обеспечивание.  
Используйте достоверные пароли. Не используйте композиции, которые просто выбрать или же угадать.  
Не открывайте почтовые инвестиции от неведомых отправителей – они имеют все шансы быть заражены вредным ПО.  
Не перебегайте по ссылкам, приобретенным по почте от неведомых отправителей или же неведомых сайтов – это раз из нормальных стезей распространения вредного ПО.  
Избегайте беззащитных сеток Wi-Fi в социальных пространствах – в их вы уязвимы для атак Man-in-the-Middle.

Вывод

Подведем выводы  
Следуйте обычным правилам, дабы гарантировать собственную защищенность и не стать жертвой интернет-мошенников.  
  
Внимательно проверяйте адрес отправителя.  
Отыскиваете информацию об промоакциях или же выплатах на официальных веб-сайтах фирм и ведомств.  
Изменяйте учетные данные не по ссылке из послания, а автономно зайдя на вебсайт.  
  
Не перебегайте по недоверчивым ссылкам.  
Не открывайте присланные файлы, в случае если не не сомневаемся в отправителе.  
Не ставьте приложения из непонятных источников.

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

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.