Эссе на тему «Проблемы кибербезопасности и пути их решения»

Нарась Олег Константинович С8119 – 10.05.01-1спец

На протяжении всей истории человечество сопровождали и проблемы сохранения и применения информации. И с появлением первых осознанных мыслительных процессов человек начал искать способы как-либо использовать свое знание для превосходства над другими людьми. Позже это вылилось в информационные войны между государствами, шпионов и т.п. Однако в 21 веке эта проблема, во многом похожая на прошлые свои проявления, все же сильно изменилась. Появилась кибербезопасность – совокупность методов, технологий и процессов, предназначенных для того то бы защитить целостность программ данных и сетей от цифровых атак. Кибербезопасность Злоумышленники производят атаки на какие-либо ресурсы или даже обычных людей с целью получить выгоду, например, шантажом, или прерыванием каких-либо производственных процессов. [[1]](https://spravochnick.ru/informacionnaya_bezopasnost/problemy_kiberbezopasnosti/) Кибербезопасность решает такие вопросы как сохранение целостности, доступности, конфиденциальности данных; безопасность программ и приложений; тестирование на проникновение; сетевая безопасность; мобильная безопасность; защита и управление доступом (идентификация, аутентификация, авторизация и т.п.); обучение пользователей, сотрудников и персонала. [[2]](http://withsecurity.ru/kiberbezopasnost-voprosy-problemy-i-ugrozy-bezopasnosti)

Киберугроза – это возможность злонамеренной попытки повредить или разрушить компьютерную сети ли систему, получить доступ к файлам и проникновения или кражи данных. [[3]](https://itsecforu.ru/2017/03/08/%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D1%8B-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D1%83%D0%B3%D1%80%D0%BE%D0%B7%D1%8B-%D1%82%D0%B8%D0%BF%D1%8B-%D1%83%D0%B3%D1%80%D0%BE%D0%B7/) Классификация на типы киберугроз включает в себя: социальную инженерию, фишинг, вирусное программное обеспечение, вирусы-вымогатели, атаки вайпер, кражу интеллектуальной собственности, кражу денег, man in the middle, ботнеты.

У киберугрозы всегда есть свой источник. Почти всегда кибератака становится возможна из-за влияния человеческого элемента, например, кто-то попался на фишинговое письмо. К источникам киберугроз можно отнести национальные государства или национальные правительства, террористов, промышленных шпионов, организованные преступные группировки, хактивистов и хакеров, деловых конкурентов, а также просто недовольных чем-то людей. Так же к источникам можно отнести и критические с точки зрения безопасности технологии, а это облачные технологии, Интернет вещей(IoT), использование личных устройств(BYOD), социальные медиа, мобильные приложения, Big data. [[4]](https://studme.org/331419/ekonomika/istochniki_kiberugroz_osnovnye_problemy)

Далеко не каждая кибератака приносит успех, большая часть из них отсеивается в почтовых сервисах в спам, а другие убирает антивирус. Но все-таки киберугрозы на 2020 год это одни из самых важных угроз для людей или компаний. Кибератаки имеют успех при атаках на какие-либо компании чаще всего из-за халатности самого руководства. Часто сотрудники отвечающие за безопасность и администрирование, а так же руководство компании просто не уделяют должное внимание таким вроде бы вещам как: Детализация трафика – если не детализировать трафик то угрозы и подозрительные процессы обнаружить становится в разы сложнее; Бесконтрольность – распыление ресурсов компании на поиск и выявление угрозы по косвенным признакам, а не предиктивное предотвращение вражеского вторжения; отказ от фильтрации сообщений, что приводит к распространению фишинговых атак; использование стороннего ПО; отказ от шифрования данных, которое будет выступать последней защитой информации которую мог бы украсть злоумышленник; слишком сильно полагаться на свою защиту думая что она достаточно совершенна что бы защитить от любых угроз, не обновляя ее. [[5]](https://habr.com/ru/article/413191/)

В России проблема кибербезопасности довольно слабо регулируется. Нормативно правовая база по кибербезопасности сформирована на основе доктрины от 2000 года [[№ Пр-1895]](http://base.garant.ru/182535/) . Существует всего 1 глава, отведенная под киберпреступления [[6]](http://base.garant.ru/10108000/42bb11d7291ec544e2ec2604179c0da1/). Так же возникают сложности с определением наказания за копирование, уничтожения или блокирования информации, так как нет четкого объяснения терминов, прописанного в законодательном уровне, что влечет за собой слишком узкий взгляд на проблему, и чаще всего для решения таких вопросов приходится привлекать специалистов что будут разъяснять сотрудникам правопорядка о той или иной проблеме. [[7]](http://www.garant.ru/article/520694/)

Глобальными причинами увеличения киберпреступлений могут выступать какие-либо катаклизмы, войны, грандиозные события, ну или как в случае с 2020 годом эпидемия Covid-19. Наравне с тем как взлетели продажи электронной техники для связи и доступа в интернет, так и выросли кибератаки на неподготовленных пользователей, незащищенные домашние компьютеры работников компаний. Те предприятия что не слишком заботились о безопасности совей работы, при выходе на дистанционный вид обслуживания, пострадали больше всего. Огромное количество сотрудников просто не обучено стандартным принципам кибербезопасности, а это приводит к тому что они работая удаленно могут успешно подвергаться кибератакам, распространяя тем самым данные которые не должны были быть похищенными. Covid-19 существенно изменит подходы к обеспечению безопасности, как изменил подход к ведению бизнеса, работе и сфере услуг. [[8]](https://www.securitylab.ru/blog/company/bitdefender/348975.php)

Для решения такой проблемы как кибербезопасность в сфере бизнеса, существует множество способов, но в общем из можно разделить на 5: Информирование и подготовка сотрудников к возможным кибератакам, создание у них грамотности в подобных проблемах; Поддержка всех уровней на которых находятся подразделения нуждающиеся в обеспечении кибербезопасности; Постоянно совершенствовать свои системы защиты, передавать специалистам из IT-отделов возможность регулировать степень защиты, а так же доступ в корпоративную сеть носителей информации или компьютеров сотрудников; Так же стоит автоматизировать процессы обеспечения безопасности, для того чтобы действительно защитить компанию, вам нужно иметь информацию о всех ваших бизнес подразделениях и конечных пользователей внутри сети, а чаще всего вручную это обеспечить не выйдет. [[9]](https://www.anti-malware.ru/analytics/Threats_Analysis/TOP_5_tips_for_cybersecurity_business)

Развитие кибербезопасности так и киберпреступности в 2020 году объективно резко выросло. Киберпреступниками стать намного проще, ведь все обучающие материалы по взлому систем доступны в открытых источниках. Но и компании стали все чаще интересоваться информационной безопасностью, проверять готова ли их инфраструктура к кибератакам. [[10]](https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019-2020/)

Я думаю, что обеспечение защиты рядовых пользователей является одним из важнейших принципов которые, помогут снизить количество успешных кибератак, а также увеличить защиту и компаний в том числе. Применяя все более новые средства защиты, мы сможем добиться определенного успеха, однако без обеспечения грамотности в вопросе кибербезопасности, обычные люди даже с хорошим щитом, все равно смогут попасться на обычный фишинг. Для того что бы в большей мере исключить подобные случаи, нужно развить в людях чувство того что их безопасность находится в их же руках, что атаки, которые, по их мнению, проводятся на какие-то абстрактные величины вроде IT компаний гигантов, так же могут коснуться и их личной информации. Я считаю, что стоит ввести у обучающихся не просто предмет, объясняющий о опасностях в сети, но и наглядно показывать, что может произойти сих данными. В 21 веке это, как я считаю был бы самый востребованный предмет в школах и вузах, а также стал обязательным знанием при устройстве на работу.

1. Проблемы кибербезопасности - <https://spravochnick.ru/informacionnaya_bezopasnost/problemy_kiberbezopasnosti/>
2. Вопросы решаемые кибербезопасностью - <http://withsecurity.ru/kiberbezopasnost-voprosy-problemy-i-ugrozy-bezopasnosti>
3. Киберугроза. Типы киберугроз - <https://itsecforu.ru/2017/03/08/%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D1%8B-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D1%83%D0%B3%D1%80%D0%BE%D0%B7%D1%8B-%D1%82%D0%B8%D0%BF%D1%8B-%D1%83%D0%B3%D1%80%D0%BE%D0%B7/>
4. Источники киберугроз - <https://studme.org/331419/ekonomika/istochniki_kiberugroz_osnovnye_problemy>
5. Причины успеха кибератак - <https://habr.com/ru/article/413191/>
6. 28 глава УК РФ - <http://base.garant.ru/10108000/42bb11d7291ec544e2ec2604179c0da1/>
7. Причины проблем кибербезопасности в России - <http://www.garant.ru/article/520694/>
8. Влияние Covid-19 на кибербезопасность - <https://www.securitylab.ru/blog/company/bitdefender/348975.php>
9. Обеспечение кибербезопасности в сфере бизнеса - <https://www.anti-malware.ru/analytics/Threats_Analysis/TOP_5_tips_for_cybersecurity_business>
10. Общие тенденции и способы улучшения кибербезопасности - <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019-2020/>
11. [№ Пр-1895] - <http://base.garant.ru/182535/>