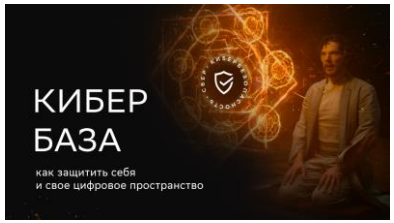
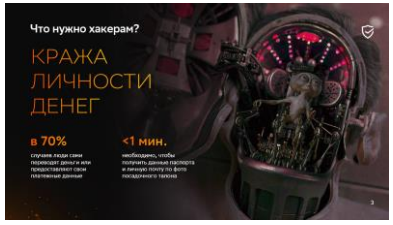
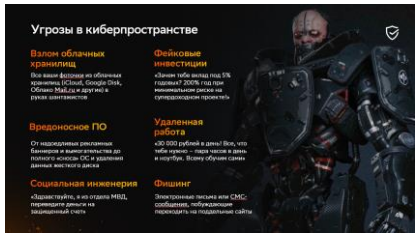
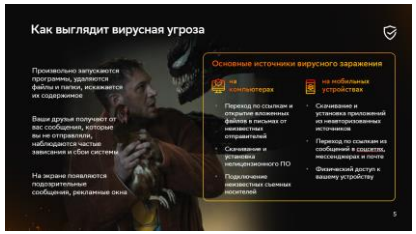
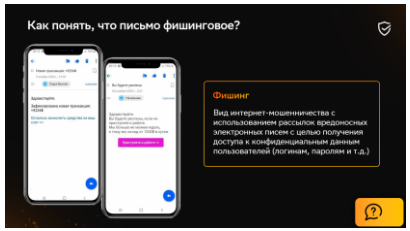
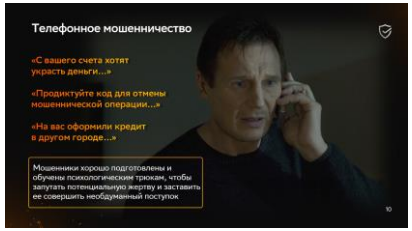
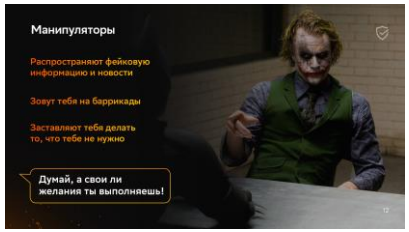
Скрипт для короткого выступления перед студентами по теме
«Кибербаза» (*базовые знания по кибербезопасности*)

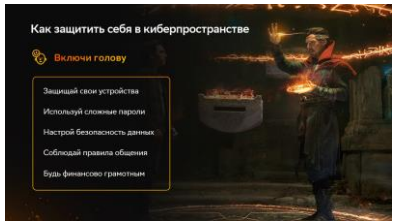
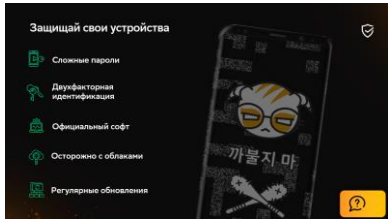
1		Добрый день, дорогие друзья. Большое спасибо, что пришли на нашу встречу сегодня. Сегодня мы поговорим об одной из наиболее актуальных современных тем: о защите себя и своих данных в цифровом мире. О чем пойдет речь в презентации: - выделим основные угрозы в киберпространстве, как цифровые, так и те, что опасны лично для вас - отдельно поговорим о конфиденциальности в Интернете - и конечно, о том, как защитить себя
2		Сегодня наше с вами качество жизни очень сильно зависит от Интернета и цифровизации. Мы работаем, общаемся, покупаем, учимся в онлайне, а технологии и цифровые услуги вокруг нас развиваются очень быстро, привлекая новых пользователей, компании и деньги. Но, к сожалению, у всего этого есть и оборотная сторона – бурный рост киберпреступности и кибермошенничества. Количество кибепреступников и киберпреступлений растет с каждым годом. Серьезные киберинциденты могут принести колоссальный ущерб людям, компаниям и государственным организациям, парализуя их работу. При этом уже много лет существует серьезный кадровый голод на специалистов по кибербезопасности. Я думаю, что вы прекрасно понимаете, что нужно кибепреступникам и мошенникам. ***ВОПРОС К АУДИТОРИИ: что же им нужно?***
3		Да, они охотятся за вашими деньгами и вашими данными, с помощью которых, опять же, кибепреступники зарабатывают деньги. К сожалению, с годами киберпреступность стала одним из наиболее прибыльных секторов теневой экономики в мире. Из-за разнообразия технологий и цифровых услуг «зоопарк» киберугроз также весьма обширен.

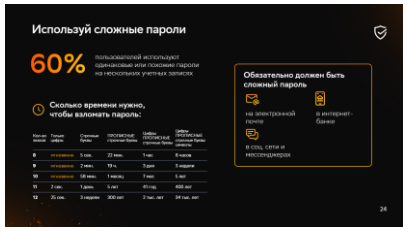
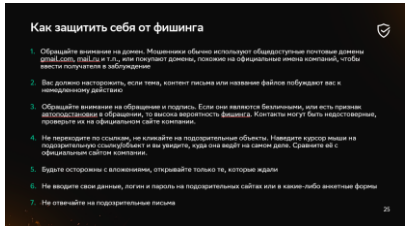
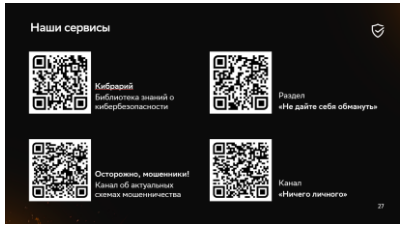
4		Рост популярности облачных хранилищ привел к тому, что злоумышленники активно пытаются их взломать для получения доступа к личной и рабочей информации для последующего шантажа и вымогательства. Я уверен, что большинство из вас не единожды слышали про вирусы и вредоносные программы. Если 25 лет назад большинство создаваемых вирусов не были нацелены на принесения нелегального дохода вирусописателям, то сегодня 99,9% вредоносных программ создаются именно с целью криминального заработка. Фейковые инвестиции и виртуальные финансовые пирамиды обещают вам баснословный доход при минимальных рисках, хотя в реальности ситуация прямо противоположная – никакой прибыли и огромный риск потерять все деньги. С телефонным мошенничеством, когда звонит «служба безопасности банка» или «следователь», как и с фишингом, сталкивались, наверное, практически все здесь сидящие. Теперь давайте поговорим подробнее о некоторых видах кибегугроз
5		Количество вредоносных программ растет с каждым годом, для злоумышленников они на протяжении многих лет являются весьма эффективным инструментов нелегального заработка. Ваши личные или рабочие файлы, ваши логины и пароли от социальных сетей, облачных хранилищ и онлайн-банка – все это всего лишь цели для вредоносных программ. А в том редком случае, если злоумышленникам нечего украсть, то они всегда могут воспользоваться ресурсами вашего устройства, включив его в состав ботнета для рассылки спама, DDoS-атак или скрытого майнинга криптовалют или же зашифровать все файлы на компьютере или смартфоне и вымогать деньги за ключ для расшифровки… И если вредоносные программы заточены под конкретную операционную систему, то фишинг – это кроссплатформенная угроза. Другими словами, для злоумышленника не имеет значения устройство, с помощью которого вы прочитаете мошенническое письмо. Для него важно, чтобы вы среагировали.

6		Именно поэтому киберпреступники стараются сделать письмо максимально привлекательным (крупный выигрыш, высокооплачиваемая работа) или максимально тревожным («ваша учетная запись заблокирована», «ваш аккаунт будет удален», повестка в суд), побудив вас совершить необдуманное действие, например, перейти по ссылке из письма и ввести ваши логин и пароль от социальной сети. Что делать в подобных ситуациях, и как вы можете распознать фишинговое письмо? Неизвестный почтовый ящик, с которого пришло письмо, зарегистрированный на общедоступном сервисе Обезличенное обращение и отсутствие контактов/подписи Обычно ссылка, по которой надо перейти, чтобы что-нибудь получить (ссылка ведет на фишинговый сайт) Содержание письма подталкивает вас к немедленным действиям, либо обещая денежные призы и подарки, либо пугая различными штрафами и санкциями. Но помимо «классического» фишинга, злоумышленники сегодня также активно используют и вишинг, или телефонное мошенничество.
7		Печальный факт – мошенничество сегодня стало индустрией. Сегодня нас с вами атакуют целые колл-центры. Прибыль одного из таких колл-центров из 20-30, так называемых, «сотрудников» может достигать в месяц порядка 75 млн рублей. Каждый из нас для них – всего лишь источник дохода. В топе схем, на которые чаще всего мы попадаемся – это перевод на безопасный, защищенный или страховой счет и оформление кредита. Самый правильный способ борьбы с подобным видом мошенничества - это просто положить трубку и не пытаться их обхитрить или троллить. Помните, что мошенники – это ещё и хорошие психологи. Онлайн-пространство сегодня огромно и привлекает не только кибепреступников и мошенников всех мастей, о которых мы уже говорили, но других опасных личностей.

8		Эти личности сидят в сети гораздо дольше вас и знают все особенности поведения молодых людей и активно этим пользуются. Будьте осторожны, если вдруг все ваши желания начинают невероятным образом осуществляться. Возможно просто кто-то очень хорошо знает, как можно эмоционально вас поймать на крючок. Вы ошибаетесь, если считаете, что вас это не касается, или что вы никогда с этим не столкнетесь.
9		Здравый смысл и скептицизм по отношению к любой информации, с которой вы сталкиваетесь в Интернете – это залог вашей личной безопасности и здоровой психики. Количество недостоверных публикаций растет лавинообразно, а слово «фейк» в последние годы плотно вошло в наш повседневный лексикон. Всегда старайтесь проверять любую информацию, которую читаете, слышите и видите. Официальные источники информации (государственные ресурсы, официальные пресс-релизы компаний), а не пикабукшечка или канал в Телеге, очень часто помогают отличить правду от вымысла.
10		Я думаю, что вы сталкивались с ситуацией, когда вы общаетесь в чате или соцсети, и вдруг появляется кто-то, кто начинает вас унижать, оскорблять и всячески провоцировать на негативные эмоции. Это могут делать целенаправленно не только с целью получения вашей негативной реакции (всегда помните о старой поговорке из Интернета эпохи нулевых: не кормите тролля / хейтера). Задача – чтобы вы заинтересовались человеком, которые вас задевает, захотели выяснить «что это за урод» и перешли в его профиль или на его страничку в соцсети. Перейдя вы увидите ссылку на другую соцсеть, мол, «меня можно найти здесь» и ссылка… Ну а перейдя по ссылке, вы попадаете на фишинговую страницу, с которой утекают ваши данные, и в дальнейшем может быть взломан ваш аккаунт. Помните, что в первую очередь вы сами отвечаете за собственную цифровую безопасность и конфиденциальность, о которой мы поговорим сейчас.

11		Все, что вы делаете в Интернет, остается в Интернете, какими бы средствами анонимизации вы не пользовались. Любое ваше действие, будь то лайк, комментарий, переход по ссылке, опубликованная фотография, формирует ваш цифровой портрет, который различные организации (как легальные, так и нет) будут пытаться монетизировать. ***ВОПРОС К АУДИТОРИИ: кто хоть раз внимательно читал пользовательское соглашение при регистрации на сайте или установке ПО?***
12		А тем временем в пользовательских соглашениях вот этих популярных соцсетей есть следующие пункты… Неправильные настройки профиля могут привести к тому, что опубликованная информация распространяется не так, как вы планировали. Простыми словами – в ВК вы даете согласие на распространение любой публикуемой информации о вас, а в ТикТоке собираются ваши данные для специальной подборки рекламы и не только. Вы можете возразить и сказать, что пользуетесь VPN, чтобы скрыть свои действия. Да, это в чем-то, может помочь, но…
13		Когда вы подключаетесь к VPN, интернет-провайдер может это заметить, но он не узнает, какие страницы вы посещали и что на них делали. VPN безопасен лишь относительно: он не гарантирует вам полную анонимность — о вашей активности в интернете будет знать сервер, к которому вы подключились, и владельцы сайтов, которые вы посещаете. VPN не защищает от хакерских атак, которые приходят извне: фишинговых писем, вредоносных ссылок или звонков мошенников. Получив доступ к устройству, хакеры могут получать любые данные, даже если вы пользуетесь VPN. Приложение любой соцсети также раскроет личность пользователя, стоит только подключиться к нему через VPN. К сожалению, некоторые сервисы VPN сегодня могут быть опасны, так как собирают информацию о вас для перепродажи, плохо защищают данные**.** Например, в ноябре 2021 года в даркнете продавали данные более 45 миллионов пользователей сервисов Free VPN и Dash VPN. База содержала данные с 2017 по 2021 годы: пароли, даты регистрации, обновления профиля и время последнего входа в систему.

		Дополнительно приложение VPN-сервиса может собирать данные о вашем местоположении, и увеличивать количество рекламы, подмешивая ее в трафик. Итак, мы много говорили про различные угрозы в киберпространстве. Теперь давайте посмотрим, как вы можете максимально себя обезопасить в цифровом мире.
14		Первое и самое главное – здравый смысл. Он – основа вашей кибербезопасности. Помните о том, что бесплатный сыр бывает только в мышеловке, установите защитное ПО на все ваши устройства, используйте сложные пароли, обязательно настройте вашу конфиденциальность на всех сайтах и сервисах, общайтесь (или не общайтесь, если не хотите) с другими так, как вы бы разговаривали в реальной жизни. Соблюдая эти базовые правила, вы обезопасите себя от большинства угроз.
15		Обязательно защищайте свои устройства и свои аккаунты. Настройте двухфакторную идентификацию, где она доступна. Это метод идентификации пользователя при помощи запроса данных двух разных типов, что обеспечивает двухслойную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения. На практике это обычно выглядит так: первый рубеж — это логин и пароль, второй — специальный код, приходящий по SMS или электронной почте. Устанавливайте на свои устройства программное обеспечение только из официальных источников (App Store, Google Play, официальные сайты производителей), так как приложения из сторонних источников могут красть ваши учетные данные и совершать другие вредоносные действия. Используйте сложные пароли (о них подробнее чуть позже) и будьте максимально внимательны при использовании облачных сервисов. Всегда устанавливайте обновления для вашей ОС и софта, чтобы получать исправления уязвимостей, которыми пользуются злоумышленники для атак. ***ВОПРОС К АУДИТОРИИ**: кто использует одинаковые или похожие пароли для всех сайтов / сервисов?*

16		Всем понятно, что очень непросто запомнить огромное количество сложных паролей для разных ресурсов, поэтому старайтесь пользоваться менеджерами паролей от надежных производителей, которые помогут вам обезопасить ваши аккаунты. Вам нужно придумать лишь один сложный мастер-пароль для самого приложения, а оно уже будет генерировать и запоминать сложные пароли для всех ваших сервисов. Если вы не хотите доверять свои пароли стороннему ПО, то обязательно создайте уникальные сложные пароли для наиболее критических сервисов: почта, госуслуги, онлайн-банкинг, соцсети и мессенджеры. Простые пароли сегодня очень быстро взламываются, и с ростом вычислительных мощностей скорость прямого подбора паролей так же растет. Несколько лет назад общепринятой рекомендацией, например, по длине пароля, было 8 символов, сегодня стандартом по минимальной длине является 12 символов.
17		Мы уже обсудили основные признаки фишингового письма, поэтому рекомендации по защите от этого вида мошенничества следующие…
18		Пройти курсы обучения, чтобы закрепить свои знания и в целом повысить свой уровень киберграмотности. Мы рекомендуем платформу «Кибрарий», на котором размещены обучающие курсы. Каждый курс займет не более 20 минут вашего времени, но поможет более детально разобраться в теме. Выбирайте курс, переходите по коду и становитесь по-настоящему киберграмотными Не держите знания в себе, активнее делитесь со своими друзьями и близкими полезными материалами. Пусть эти памятки сохраняться у вас в телефоне и помогут лучше запомнить правила кибербезопасности…