**По материалам сайта**

[**https://www.sb.by/articles/kibervoyny-kak-vystroit-oboronu.html**](https://www.sb.by/articles/kibervoyny-kak-vystroit-oboronu.html)

**Беларусь надежно защищена от цифровых угроз,**

**но это сфера постоянного внимания**

**Кибервойны: как выстроить оборону**

Наша страна надежно защищена от цифровых угроз, но работы в этом направлении должны вестись постоянно.

Во всем мире количество кибератак из года в год растет. Преступники прицельно бьют по инфраструктуре, останавливая работу предприятий. После чего требуют выкуп, чтобы восстановить систему. Правда, не всегда их действия связаны с наживой. Есть и политически мотивированные взломщики. Как противостоять информационным угрозам?



Александр Лукашенко:

*– Во всем мире (может быть, для нас так не характерно, но тем не менее факты имеют место быть) рост наблюдается кибератак. Причем атакуют прежде всего стратегические объекты, государственные органы, предприятия, банковскую систему. Цель — нанести максимальный ущерб экономике и дестабилизировать в итоге общество. Следует обезопасить наше государство с учетом того, что у нас есть. Давайте будем исходить из того, что цели мы определили, знаем, что такое кибервойна, что такое кибербезопасность. Все это в нашей Концепции национальной безопасности прописано. Дальше мы должны понимать и понимаем, на что будет направлена кибератака. Нужно создавать систему безопасности на тех объектах, которые будут атакованы в случае кибервойны.*  
25 октября 2022 года, на совещании по теме кибербезопасности во Дворце Независимости.

**Ключ без права передачи**

В нашей стране работа в сфере виртуальной безопасности находится на высоком уровне. Тем не менее довольно крупные суммы порой утекают в руки злоумышленников из-за банальной невнимательности самих сотрудников предприятий. К примеру, минскую компанию обчистил один «умелец». Он отправил на электронную почту письмо, в котором содержался файл с вредоносным программным обеспечением. Главный бухгалтер опрометчиво его открыл. Компьютер оказался зараженным. Потом злоумышленнику удалось перевести около 50 тысяч рублей со счета организации на счет своего подельника. Через подставное лицо деньги удалось обналичить.  
*– Во многих организациях бухгалтеры просматривают десятки электронных сообщений в день. Это могут  быть и реклама, и важные финансовые документы, и даже ошибочно направленная корреспонденция. Поэтому когда сотруднику попадается письмо, например с названием «финансы», велики шансы, что он его откроет. А дальше дело техники – установочный файл автоматически распаковывается и заражает компьютер вирусом, —* рассказывает официальный представитель управления Следственного комитета по Минску Екатерина Гарлинская.*— Как правило, бухгалтер всегда очень загружен и не извлекает электронный ключ системы «Клиент-Банк» из компьютера часами. Обед, поход к начальнику и любая причина отсутствия на месте – это «прекрасная» возможность для злоумышленника получить доступ к счетам организации.*  
 В практике столичных следователей есть случай, когда в течение дня на счете отсутствовали средства, но в этот же вечер на него поступило 30 тысяч рублей. На следующее утро злоумышленникам удалось обнулить счет.

**Расшифровка обходится дорого**

Бывает,  бизнесмены становятся жертвами третьих лиц, которые умело вклиниваются в электронную переписку. Такой случай произошел в сентябре в Клецком районе. Агропредприятие вело диалог с польской компанией о покупке техники. В итоге, когда дело дошло до перевода денег, 300 тысяч рублей ушли мошенникам. Они взломали почту белорусской конторы и увели переписку на другой электронный ящик.

Еще один способ атаки — посредством вирусов-шифровальщиков. Они тоже приходят по электронной почте. Заместитель начальника главного управления по противодействию киберпреступности МВД Беларуси Александр Рингевич отмечает, что у нас 16 организаций из-за шифровальщиков потеряли деньги:

*– Но это не целенаправленные и подготовленные атаки, к примеру, как на бразильскую мясопроизводящую компанию JBS или американскую Colonial Pipeline. У нас мы имеем дело с веерной рассылкой.*

Как это работает? Любая информация стоит денег. Виртуальные аферисты собирают базу корпоративных почт, продают ее на теневых ресурсах. Дальше в дело вступает тот, кто их покупает. Он организовывает массовую рассылку с одинаковым текстом сообщения и прикрепленным файлом. Если на него кликнуть, запускается опасный вирус. В итоге цифровая информация предприятия кодируется, и, по сути, фирма берется в заложники. Стоит ли платить вымогателям? Александр Рингевич рекомендует:

*– Мы советуем пострадавшим написать на электронную почту, с которой пришло письмо. Но в 80 % случаев ответов нет: либо электронный ящик заброшен, либо заблокирован, либо больше не используется. А суть в том, что они ведь не знают, какой компьютер конкретно нужно расшифровать. И как дадут ключ? А если обратной связи нет, платить не имеет смысла.*



**Масштабный подход**

Самые распространенные атаки сегодня совершаются при помощи социальной инженерии, отмечает заведующий кафедрой телекоммуникаций и информационных технологий факультета радиофизики и компьютерных технологий БГУ Юрий Воротницкий:

*– Среди объектов этих атак много госучреждений, в том числе медицинских, образовательных. Также удары прицельно наносятся по промышленным компаниям.*  
Заведующий кафедрой защиты информации БГУИР Тимофей Борботько вспоминает глобальные хакерские «обстрелы», последствия которых сказались не только на фирмах, но и на простых гражданах:  
*– В прошлом году американцы из-за атаки на оператора крупнейшего в США трубопровода Colonial Pipeline ввели чрезвычайную ситуацию. Виной тому — вирус-шифровальщик. Зараженной оказалась корпоративная сеть.*

В результате приостановка работы трубопровода на несколько дней спровоцировала нехватку бензина.

*– Первое, на что нацелены такие атаки, – это вывести компанию из строя,*– продолжает эксперт. *– Если организация использует свою информационную систему для управления технологическими процессами, то вмешательство в эти процессы может привести к тому, что предприятие перестанет работать. А пока ты на рынке отсутствуешь, твое место занимают конкуренты. Это один из вариантов развития событий.*

Политическая ситуация также влияет на то, кем заинтересуются хакеры. По данным МВД, в 2020 году на наши предприятия атак было в три раза больше, чем в 2019-м. Показательная ситуация — в России. Там после начала СВО в 3—5 раз увеличилось количество киберударов с помощью так называемых вайперов (безвозвратно шифруют все данные). Здесь цель — нанести ущерб, говорит Тимофей Борботько:

*– Нарушители могут вывести из строя те предприятия, которые приносят в бюджет неплохую прибыль. И тогда плохо будет всем.*

В этом контексте понятно, почему Президент уделяет цифровой защите огромное внимание. 25 октября на совещании по теме кибербезопасности Александр Лукашенко поставил задачу обеспечить безопасность важных объектов на случай, если они подвергнутся кибератакам. Но при этом не создавать для реализации этих задач дополнительные структуры.  
 Начальник Оперативно-аналитического центра при Президенте Андрей Павлюченко, говоря о разработке национальной концепции кибербезопасности, отметил, что Глава государства поручил детально проработать документ в этой сфере, для того чтобы он был системным и масштабным, охватывал различные сферы и отвечал современным вызовам и угрозам. В ОАЦ выполнением поставленной задачи будут заниматься центр компетенций и квалифицированные специалисты.  
 **Утечка до уголовного дела доведет**

Еще один бич современности — утечка персональных данных из закрытых баз данных. Несоблюдение организациями мер по обеспечению защиты персональных данных становится основной ее причиной, говорит заместитель начальника управления контроля и аудита Национального центра защиты персональных данных Виталий Диско:  
*– Центр практически каждую неделю фиксирует информацию об утечке персональных данных в различных сферах. Наиболее часто такие инциденты затрагивают сферу торговли, включая продажу товаров через интернет, либо организации, которые занимаются оказанием услуг в интернете и ведут базу данных своих клиентов.*

Когда становится известно об утечке, сотрудники центра в первую очередь требуют сообщить об этом тем, чьи данные попали в сеть. Если там есть пароли, то следует изменить их.  
*–  Далее мы обращаемся к владельцам соответствующих интернет-ресурсов, где опубликована такая информация, с запросом об ее удалении, —* объясняет специалист. *— Несмотря на то что взломанные базы данных публикуются в зарубежном сегменте сети интернет, наши требования, как правило, удовлетворяются, поскольку распространение персональных данных без согласия — это противоправное деяние не только у нас, но и в других государствах, в том числе в России и  странах Европы. Параллельно с этим ведется работа с оператором по устранению последствий инцидентов и выстраиванию модели защиты персональных данных в организации.*

Что касается ответственности за инфоутечку, руководителю организации, где это произошло, может грозить уголовная ответственность. Задумываться о защите персональных данных — забота не только государства, но и компаний и рядовых граждан.

Александр Вольфович, Государственный секретарь Совета Безопасности:

*– Вопросы кибербезопасности приобретают сегодня наибольшую актуальность, и еще неизвестно, что страшнее: киберугроза или развязывание военной агрессии. В случае военной агрессии — гибель людей, а здесь гибель целых инфраструктур, государственных институтов, которые могут вызвать гибель того или иного государства без выстрелов или других видов воздействия.*  
 *Недавно состоялось совещание у Президента Беларуси, где были доложены вопросы, связанные с развитием кибербезопасности на территории нашей страны. Дан ряд указаний, в ближайшее время, думаю, появится указ о вопросах кибербезопасности. Конечно же, этим вопросам уделяется самое пристальное внимание, идет обмен мнениями, взаимодействие с Россией. Мы смотрим, перенимаем опыт у Китая, других стран по этим вопросам.*

**Код анализа**

В управлении «К» МВД с начала года зарегистрировано 12,5 тысячи киберпреступлений. 70 % из них на удивление — звонки «банковских работников». Александр Рингевич отмечает, что «банкиры» активно обманывали людей с начала года до середины февраля, затем на первый план вышли мошенничества на торговых площадках. Сейчас снова звонки набирают обороты:  
—  Такая тенденция напрямую связана с политической обстановкой в Украине. Именно оттуда поступают практически все звонки. Как только началась спецоперация, сразу же произошел резкий спад звонков так называемых банковских работников.

К слову, если раньше эти аферисты требовали у людей данные карточки, то сегодня просят назвать код, который придет из банка на телефон для отмены несанкционированной операции по счету. И после этих слов человек видит сообщение. Пазл складывается:  
*– Только назначение пришедшей информации другое. Преступники говорят, что это код для отмены операции, а на самом деле это код для внедрения дополнительного устройства в свой интернет-банкинг. Таким образом человек добровольно пускает мошенников в свой «кошелек». Еще просят установить приложение для дистанционного управления.*

Вообще, злоумышленники могут наплести что угодно. Так, сотрудник одного из госпредприятий думал, что помогает техническому специалисту из центрального офиса проводить тестовые платежи в Россию: за три часа телефонного разговора за границу ушло 45 тысяч рублей.

Денис Карась, член Постоянной комиссии Палаты представителей Национального собрания Беларуси по промышленности, топливно-энергетическому комплексу, транспорту и связи:  
*– Такое понятие, как «кибербезопасность», отражается в различных нормативных документах. Созданы структуры, которые занимаются вопросами защиты информации. В их числе — Центр защиты персональных данных. Основной регулятор в этом вопросе — Оперативно-аналитический центр при Президенте. Помимо этого, функцию Министерства цифровизации выполняет Министерство связи. У нас в стране есть Государственная программа «Цифровое развитие Беларуси» на 2021—2025 годы.*

К слову, сейчас в рамках Союзного государства принято 28 союзных программ. Из них порядка восьми касаются цифровизации. Вместе с тем риск всевозможных угроз возрастает. Поэтому мы понимаем, что, прежде чем внедрять эти системы, нужно продумать, как их защищать.  
 В прошлом году прошла встреча с представителями компании «Белорусские облачные технологии». Так вот на них ежедневно совершалось до нескольких сотен кибератак. Но у них наработана система безопасности. А представьте, что произошло, если бы та информация, которая хранится у них, попала в руки хакеров.

**Не купиться на подделку**

Подготовились проходимцы и к сезону «черных пятниц» – создали  много сайтов-подделок, копирующих оригинальные интернет-магазины. Цель этих ресурсов — кража денег и данных банковских карт.

*– Такое направление мошенничества называется «скам», то есть продать несуществующий товар или услугу. Человек видит скидки и теряет разум. К тому же поддельные сайты визуально мало чем отличаются от оригинала,*–  говорит Тимофей Борботько.

Киберворы используют те же каналы продвижения, что и легальные ресурсы: рассылку в мессенджерах, поисковую оптимизацию и продвижение в соцсетях. При этом покупают доменное имя со схожим названием, отличие будет в несколько символов:

*– При совершении онлайн-покупок нужно обращать внимание на адресную строку. И платежи осуществлять с открытой специально для этих целей карты. Также желательно скачать на смартфон платный антивирус. Он проверяет веб-ссылки, URL-адреса и многое другое. Ведь рядовой пользователь не разбирается в этом и не собирается этого делать.*

**Профессия на вырост**

В следующем году в БГУ начнут готовить кадры в области кибербезопасности. Об этом рассказал заведующий кафедрой телекоммуникаций и информационных технологий факультета радиофизики и компьютерных технологий БГУ Юрий Воротницкий:

*– Я думаю, у многих появляется вопрос, почему классический вуз будет заниматься подготовкой таких специалистов. Во-первых, задача обучения кибербезопасности – междисциплинарная. Потому что, с одной стороны, те, кого мы будем готовить, должны владеть фундаментальными знаниями математики, физики и информатики, методами и средствами защиты информации и информационно-коммуникационной инфраструктуры, основанными на знании математических и радиофизических методов, криптографии, электроники и схемотехники. Это то, что касается технической защиты информации и инфраструктуры, обеспечивающей ее передачу, прием, хранение и обработку. Но кибербезопасность предполагает еще и применение организационных и правовых мер. Нужно иметь знания по психологии, управлению коллективом, коммуникациям. Хороший специалист должен владеть основами расследования киберпреступлений. Все эти знания в комплексе как раз и может дать классический университет. Кроме того, специалист в области кибербезопасности должен уметь организовывать работу по защите информации на предприятии.*

Сейчас преподаватели вуза активно встречаются с потенциальными работодателями, чтобы те помогли выработать четкие требования к специалистам. Помимо этого, важно наладить диалог с компаниями для того, чтобы студенты проходили там практику и имели в будущем возможность распределиться.