ТЕХНОЛОГИИ
03 НОЯБРЯ 2025, 18:15

Путь самурая, стрессоустойчивость и уязвимости: как в Беларуси готовят безопасников?

НОВОСТИ ТЕМЫ **"ПРОЕКТ "В ТЕМЕ" НА YOUTUBE-КАНАЛЕ БЕЛТА"**

"Необходимо введение диктатуры!" Политолог про оптимальный стиль власти для США
Реально работающая профилактика: что делать, чтобы уберечься от болезней легких?

Почему специалиста по кибербезопасности сравнивают с самураем? Что делает безопасник в организации и почему его работа не всегда видна? Есть ли спрос на профильных выпускников БГУИР? На эти и другие вопросы проекта компании А1 и БЕЛТА "В теме. Технологии" отвечает заведующая кафедрой защиты информации БГУИР Ольга Бойправ.

https://youtu.be/E-aloUXLkN4

- Понятие "кибербезопасность", как мне кажется, в последнее время стало размываться. Фактически из каждого утюга нам говорят, как это важно, нужно, что надо соблюдать определенные правила и так далее.

На мой взгляд, у граждан уже немного замылилось восприятие: "Ну вот опять говорят. Да мы и так все знаем". А знаем ли мы?

- Хочется надеяться, что да, уже знаем. Мне кажется, это понимание не с бухты-барахты появилось, мы к нему методично двигались. Не случилось так, что проснулись и поняли: "Да, нужно защищать информацию в цифровом мире".

Сейчас, грубо говоря, волна хайпа вокруг проблем, связанных с кибербезопасностью. Считаю, что это на пользу, потому что позволяет правила безопасного поведения в цифровом мире, скажем так, возвести в ранг правил дорожного движения. Ведь кибербезопасность важна не только для тех, кто работает в соответствующих сферах, она должна обеспечиваться в каждом доме, в каждой семье. Люди знают, что на красный сигнал светофора дорогу переходить нельзя. Постепенно в обществе формируется понимание, что надо бы подумать, прежде чем заполнить веб-формы, проверить достоверность ресурса, к которому обращаешься, и так далее.

Но это процесс, который требует времени. И как раз благодаря разговорам, распространению сведений по всем возможным каналам этого можно достичь. С недавних пор специалистов по кибербезопасности любят сравнивать с самураями: у них, как известно, нет цели, но есть путь. То же самое и с обеспечением безопасности - это движение.

- То есть это дорога, которая не имеет конца, да?

- Да. И которая, пожалуй, имеет весьма размытое начало, потому что у каждого по-своему приходит понимание.

- Преподаватель видит изменения в обществе через студентов, да?

- Конечно.

- Я очень хорошо помню своих преподавателей. Много лет прошло, спрашиваю: "Ну как?" - "Ой, студенты нынче пошли… Они другие, не те, что были вы. Вы знали это, они не знают". Это особенности времени. Вы можете отследить подобные тенденции? Вот говорите, что мы стали потихонечку привыкать к этим правилам. Студенты сегодня приходят к вам уже более подготовленные, знающие что-то? Или же, как энное количество лет назад: "Здравствуйте, я просто хочу".

- "Я готов забыть все, чему меня научили в школе". В контексте вопросов, связанных с проблемами кибербезопасности, я считаю, что с каждым годом

студенты лучше понимают, кем они хотят работать и с чем будет связана их будущая профессиональная деятельность. Вот это неплохо. Единственная наша задача как преподавателей - дать понять, что информационная безопасность - это не только про цифровое пространство, но еще и про защиту персональных данных (как своих, так и чужих). Защита информации, которая передается на бумажных носителях. Тайна тех же переговоров, которые могут проводиться в помещении, где никакое оборудование не стоит и не используется.

- Но есть хороший товарищ, который всем все расскажет.

- Это плоскость социальной инженерии. У нас на первом курсе, буквально в первом семестре, читается дисциплина "Социально-психологические аспекты информационной безопасности". Нам действительно нужно дать понять студентам, что информационная безопасность начинается с человека.

Существует стереотип, что специалист по кибербезопасности - это типичный айтишник-интроверт, который с чашкой чая сидит за компьютером и пишет программный код.

- В данном случае должно быть наоборот.

- Конечно. В данном случае безопасник должен быть, извините за грубость, душой компании, душой организации.

- Хороший опер.

- По сути, да. Вплоть до умения понимать, кого и что именно беспокоит. Потому что классика жанра - когда сотрудника, который чем-то недоволен, подкупают, и он с удовольствием делится знаниями о специфике деятельности организации. Вот с такого начинается информационная деятельность.

- Но продолжается же и более техническими вещами?

- Конечно.

- На глазах все меняется, и технологии тоже. Появляется новое устройство, а уже через полгода оно устаревает если не физически, то морально. И так далее. Как быть со студентами? Какой теперь срок обучения?

- Первая ступень - четыре года.

- За четыре года программное обеспечение, какие-то технические вещи, грубо говоря, чаще всего устаревают. Как уловить то, что надо точно дать студенту, чтобы он вышел с современными знаниями?

- Прежде всего должно быть понимание, что нужно сделать, чтобы обеспечить кибербезопасность в частности и информационную безопасность в целом. Есть хрестоматийные принципы, скажем так, аппаратно и программно независимые. Главное - сформулировать цель, к которой должен вести нескончаемый путь самурая. А уже инструментарий для достижения этой цели в каждой организации может быть свой.

Конечно, в учебном процессе мы используем продукты, которые предоставляют наши партнеры и вендоры в сфере информационной безопасности. Они стремятся, чтобы в учебном процессе мы применяли актуальные версии этих программных продуктов. Более того, не скупятся, чтобы актуализировать их.

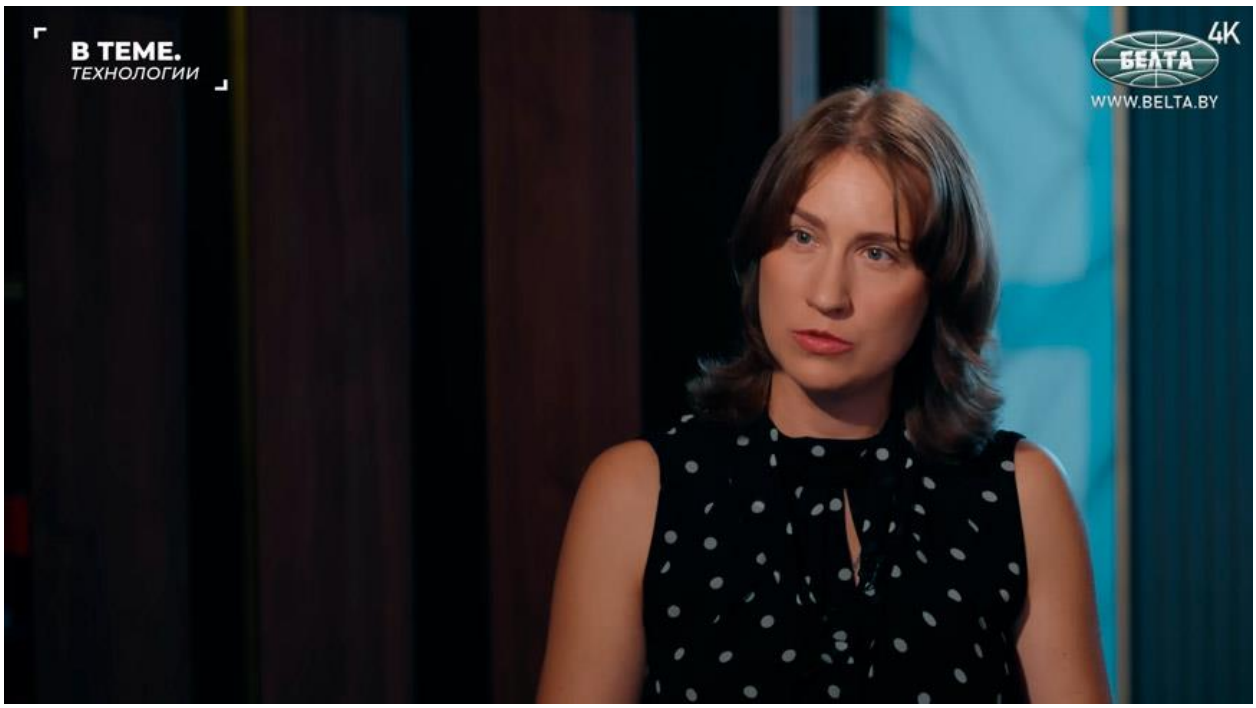
Понятно, что рынок расширяется. Но еще раз отмечу, что базовые хрестоматийные принципы остаются. А это управление уязвимостями в информационных системах, иными словами - поиск в них слабых мест. То, собственно, с чего и должна кибербезопасность начинаться. Когда киберпреступник планирует атаку, что он ищет? Слабые места, точки воздействия. Одна из задач, которая решается в этом поиске, - сбор информации о том, какое ПО используется в информационной системе организации. А уж если известно, какое оно, можно понять и слабые места.

Ключевая базовая задача безопасника - эти уязвимости своевременно закрывать. То, что об уязвимости известно, не значит, что она закрыта, следует предпринимать действия. Есть достаточно понятные алгоритмы. Нужно взаимодействовать с поставщиком используемого программного обеспечения, который обновляет продукт, чтобы не только расширить его функционал, но и "закрыть дыры", как любят говорить безопасники.

Это понимание у студента должно быть сформулировано, равно как и понимание того, что надо бы антивирусную защиту наладить в информационной системе. Алгоритмы функционирования таких программных средств плюс-минус схожи. Поэтому, если мы обучим тому, как работают антивирусные программные средства различных типов, дадим практические примеры на конкретном программном обеспечении, в перспективе, когда человек выйдет на работу, он будет готов подтянуть знания под те программные продукты, которые в данной организации применяют.

- Насколько котируются сегодня на рынке труда в Беларуси (возможно, и за рубежом) люди, которые выходят из ваших стен специалистами с дипломами?

- Отвечу про то, как они котируются у нас в стране, потому что есть задача распределить специалистов. К счастью, мы с ней справляемся для себя успешно. Для заказчиков кадров - может, не совсем. Честно говоря, не всегда можем удовлетворить все заявки, которые приходят на специалистов. На данный момент их больше, чем наших специалистов. Мы пытаемся это компенсировать, второй год подряд на 30% больше набираем, чем в предыдущие годы. Вообще кафедра защиты информации в БГУИР существует с 2005 года, ей уже 20 лет - уже даже не подросток.



- Только ваш вуз готовит таких специалистов?

- Нет. Подготовка специалистов по информационной безопасности еще проводится на базе Белорусского государственного университета, Гродненского государственного университета и Полоцкого государственного университета.

- И всех-всех-всех все равно не хватает.

- Из опыта общения с заказчиками кадров скажу, что им нужно больше. Но мы стараемся найти баланс.

- Не случится ли такая история: как милиционер должен сидеть чуть ли не под каждым кустом, так теперь возле каждого компьютера требуется специалист по безопасности? По мнению руководителей каких-то больших структур.

- Пока не просматривается такая тенденция, потому что не все руководители готовы тратиться на информационную безопасность в той степени, в которой нужно. Не всегда работа безопасника видна. Грубо говоря, когда состояние здоровья хорошее, кажется, что так и должно быть, никакие усилия не затрачиваются. Если в организации один безопасник тянет благополучно все задачи, то кажется, что у него работы на самом деле и нет. А это методический труд.

- Рутинная, достаточно скучная в чем-то работа?

- Не скажу, что скучная, потому что изощрения касательно кибератак с

каждым днем преобразуются. Изменяется логика кибератак, и это заставляет, мягко говоря, не отдыхать мозгами. Требуются определенная усидчивость и концентрации - это точно.

На мой взгляд, хорошо проводить профотбор даже на уровне психологического тестирования. Думаю, не каждый имеет склонности к работе специалистом по информационной безопасности.

- Мне очень понравилось ваше сравнение правил поведения в сети, в том числе безопасного поведения, с ПДД. По вашей оценке, "правила дорожного движения" у нас в Беларуси насколько совершенны сегодня?

- Вы имеете в виду законодательство?

- Да.

- В целом наш законодатель в сфере технической криптографической защиты информации - Оперативно-аналитический центр при Президенте Республики Беларусь. Он разрабатывает требования и актуализирует их достаточно часто. Движение есть, самурай свой путь не прекращает, скажем так.

Особенность, которая подчеркивает развитие деятельности в сфере кибербезопасности, связана с созданием киберцентров, в том числе с созданием республиканского киберцентра. Фактически это структуры, которые отвечают за поиск в журналах событий информационных систем аномалий, указывающих на то, что на систему планируется атака либо кто-то в ней уже присутствует со стороны внешних нарушителей. Можно сказать, это первая базовая компетенция для специалистов по кибербезопасности.

- Если продолжать аналогию с ПДД, на аварийно-опасном участке дороги лучше предпринять какие-то инженерные, ну если совсем ничего не получается - технические, меры? Как минимум поставить инспектора, чтобы люди его видели и ехали аккуратненько?

- Да.

- То есть здесь тоже так можно?

- Получается, так. Благодаря наличию регулятора, который может не только задать правила игры как таковые, но и подсказать, сориентировать, как их можно лучше реализовать, можно предотвратить столкновение, если не выходить из плоскости аналогии.

- И сделать так, чтобы путь самурая был прямым, а не извилистым.

- Либо хотя бы не прекращался. Если кибератака крайне успешна для преступника, иной раз безопасник может сложить полномочия и сказать: "Пойду картины рисовать. Это не для меня". В этой работе есть ситуации, где важна стрессоустойчивость.

- Пожелаем стрессоустойчивости вообще всей системе, призванной стоять на страже наших интересов. Любое киберпреступление, даже если оно совершено в отношении большого предприятия или какой-либо структуры, все равно отражается на всех.

- Конечно.

- Спасибо большое вам за разговор, Ольга, и за то, что вы думаете над тем, как путь самурая продлить и сделать его красивым.

- Это важно в любой работе, и работа безопасника не исключение. Мы стараемся. Спасибо вам.

| Подготовлено по видео БЕЛТА. Скриншоты видео.