Тезисы

Мошенничество и киберпреступность

Аннотация:

В статье рассматриваются основные тенденции развития киберпреступности как одной из разновидности экономической преступной деятельности.

Исследованы основные группы киберпреступлений и их воздействие на деятельность компаний.

Определены основные направления борьбы с киберпреступностью, предложены механизмы совершенствования

законодательства.

Ключевые слова:

сети; угрозы; киберпреступность; кибер-безопасность; киберпреступность; хакер; кибератака; глобализация; глобальная сеть Интернет; информационно-коммуникационные технологии; экономическая преступность.

1. Любые информационные и технические новации значительно расширяют сферу киберпреступности.

В отличие от других видов экономической преступности, киберпреступность в настоящее время является наиболее быстрорастущим сегментом, что связано с увеличением численности пользователей компьютеров, подключенных к глобальной сети Интернет, постоянным повышением уровня профессионализма киберпреступников, устойчивым развитием и совершенствованием информационных технологий. Любые информационные и технические новации значительно расширяют сферу киберпреступности и создают условия для повышения эффективности хакерских атак, поэтому киберпреступность растет более быстрыми темпами, чем все другие виды преступности.

Так, уровень киберпреступности повысился с 24% в 2014 г. до 32% в 2016 г., заняв вторую позицию среди видов экономической преступности в мире, опередив отмывание денег, коррупцию и другие составляющие.

2. Очевидность совершения преступных действий не всегда явная, могут совершаться совершенно скрытно.

Киберпреступления ввиду их относительной ненаказуемости, а также высокой доходности являются достаточно привлекательным видом деятельности. Риски и издержки при совершении киберпреступлений равны рискам и издержкам при осуществлении легальной трудовой деятельности (производственный травматизм, монотонность трудовой деятельности, стрессы, риск сокращения и т.д.). Распространение интернета привело к устранению национальности киберпреступности, сделало ее подлинно интернациональной. Хакер может иметь гражданство одной страны, находиться на территории другой и при этом работать через сервер, расположенный в третьей стране.

Очевидность совершения преступных действий не всегда явная, могут совершаться совершенно скрытно, в результате пострадавшая сторона узнает об этом через достаточно большой промежуток времени. Место нахождения преступника и факт совершения преступных действий, сбор доказательств являются затруднительными для правоохранительных органов, осуществления процессуальных действий.

Продолжительность самих атак при этом варьируется в достаточно большом временном интервале: от нескольких секунд до суток и месяцев.

3. Достаточно легкой жертвой киберпреступности являются предприятия малого и среднего бизнеса

Рост киберпреступности связан преимущественно не с крупными предприятиями, а именно с предприятиями МСБ. Такие предприятия в силу малого бюджета, отсутствия квалифицированных кадров, пробелов в познаниях сотрудников не могут на должном уровне обеспечить качественную информационную безопасность.

Для больших компаний, в отличие от малого и среднего бизнеса, защита конфиденциальной информации, интеллектуальной собственности имеет принципиально важное значение для успешного ведения бизнеса и требует разработки комплексной стратегии безопасности, исходя из целей деятельности компании.

4. Интернет-банкинг по-прежнему остается одним из лидеров в перечне киберпреступлений.

Электронные технологии, с одной стороны, снизили себестоимость оказываемых услуг, с другой стороны, расширение применения данных технологий увеличило возможности киберпреступников в совершении незаконных финансовых операций, что повысило риски обеспечения финансовой безопасности в банках. Преступники обогащаются за счет кибер-шантажа, вымогательства, снятия денежных средств со счетов клиентов банка.

Распространению киберпреступности в банковской сфере способствует использование банками устаревших технологий, не способных противостоять преступникам.

5. Заключение

Киберпреступность прошла фазу становления, «детства» и перешла на принципиально новый уровень, включающий вымогательство, промышленный шпионаж, таргетированные атаки.

Изменился и сам хакер: из любителя превратился в профессионала, являющегося частью криминального бизнеса. Киберпреступники наносят значительный ущерб как отдельным гражданам, организациям, предприятиям, так и всей национальной экономике при минимальном для себя риске.

Злоумышленники идут на несколько шагов вперед, увеличивая отрыв от систем безопасности компаний. Решение же проблемы киберпреступности состоит не в подстраивании компаний под существующие тенденции, а в активной разработке информационной безопасности стратегии предприятий на опережение.