МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
Дальневосточный федеральный университет

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра информационной безопасности

О Т Ч Е Т

о прохождении учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики

Выполнил студент
гр. С8118-10.05.01-1Спец
_____ Бондарь А.Е.
(подпись)

Отчет защищен с оценкой

_____

_____ С.С. Зотов
(подпись) (И.О. Фамилия)

« 31 » июля 2021 г.

Руководитель практики
Старший преподаватель кафедры
информационной безопасности ШЕН

_____ С.С. Зотов
(подпись) (И.О. Фамилия)

Регистрационный № _____

« 31 » июля 2021 г.

_____ Е.В. Третьяк
(подпись) (И.О. Фамилия)

Практика пройдена в срок
с « 19 » июля 2021 г.
по « 31 » июля 2021 г.

на предприятии
Кафедра информационной безопасности ШЕН ДВФУ

г. Владивосток
2021

Оглавление

Задание на практику

- Проведение исследования в области мошенничества и киберпреступности.
- Написание отчета по практике о проделанной работе.

Введение

Учебная (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практика проходила на кафедре информационной безопасности ШЕН ДВФУ в период с 19 июля 2021 года по 31 июля 2021 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности, а также навыков оформления проведенного исследования в отчетной форме.

Задачи практики:

1.Ознакомиться с понятием киберпреступность.

2.Теоретически ознакомиться с тенденциями развития киберпреступности.

3.На основе полученных знаний написать отчет по практике о проделанной работе.

Противодействие мошенничеству и киберпреступности

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.

Тезисы

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

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

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

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

Введение:

Одной из современных тенденций развития мировой экономики является активизация экономической преступной деятельности. Экономическая преступность превратилась в одну из наиболее важных проблем, стоящих перед человечеством, оказывая негативное развитие как на экономику отдельных государств, так и устойчивое развитие мировой экономики. Одной из составляющих многогранного понятия экономической преступности является киберпреступность, ставшая негативным последствием развития информационных технологий. Интернет используется преступными группами уже не только как вспомогательное средство, но и как место и основное средство совершения традиционных преступлений мошенничества, краж, вымогательств.

Целью исследования является анализ влияния информационных и коммуникационных технологий на состояние и тенденции развития киберпреступности в условиях глобализации мировой экономики, а также эффективности борьбы с ней.

Развитие киберпреступлений

Киберпреступность - это следствие глобализации информационно-коммуникационных технологий и появления международных компьютерных сетей.

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. По данным Международного союза электросвязи (МСЭ), являющегося ведущим учреждением Организации Объединенных Наций в области информационно-коммуникационных технологий, если в 2000 г. Число пользователей Интернета составляло 400 млн чел., то в настоящее время в мире насчитывается 3,2 млрд. В период с 2000 по 2015 г. удельный вес пользователей интернета увеличился почти в семь раз − с 6,5 до 43% мирового населения.

По данным Всемирного обзора экономических преступлений PricewaterhouseCoopers (PWC) за 2016 г., на фоне небольшого снижения экономической преступности в целом киберпреступления показали самый высокий показатель за весь период публикации обзоров.

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. (Проводимый криминологический анализ базируется лишь на данных учтенной преступности, не касаясь глубинных социальных, экономических, политических, демографических, организационных и иных причин киберпреступности).

Что из себя представляют хакеры

Кроме трансформации самой киберпреступности, меняются также и характеристики хакера: если первоначально это были люди, обладавшие знаниями, умениями, направлявшие свои действия не столько на противозаконные цели, сколько на поиск нового, то в настоящее время за преступными действиями стоит криминальный бизнес.

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.

Малый и средний бизнес

Произошла определенная переориентация направленности киберпреступности на получение преимущественно финансового результата. В отличие от распространения вирусов, направленных на создание бот-сетей (распространение ботнетов-сетей инфицированных компьютеров), осуществляющих атаки независимо от пользователей, причиняющих ущерб большому количеству пользователей, целевые атаки хакеров ориентированы на конкретное предприятие или конкретного пользователя.

Достаточно легкой жертвой киберпреступности являются предприятия малого и среднего бизнеса (МСБ). 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. Тем более, что потеря данных или же их компрометация не влияют существенным образом на их функционирование, положение на рынке, уровень доверия потребителей, наконец, размер получаемой прибыли.

Большие компании, в отличие от малого и среднего бизнеса, не могут позволить себе пренебрежительное, эпизодическое внимание к информационной безопасности в силу необходимости увеличения привлекательности, поддержания должного уровня операционной эффективности бизнеса, постоянного конкурентного давления со стороны рынка. Защита конфиденциальной информации, интеллектуальной собственности имеет принципиально важное значение для успешного ведения бизнеса и требует разработки комплексной стратегии безопасности, исходя из целей деятельности компании.

Интернет-банкинг

Интернет-банкинг по-прежнему остается одним из лидеров в перечне киберпреступлений. Банковские учреждения, независимо от времени и технических достижений, являются привлекательной целью для быстрого получения богатства.

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.

Незаконное получение реквизитов банковских карт осуществляется злоумышленниками при осуществлении владельца денежных средств различных финансовых операций с помощью электронного банкинга, с SIM карт мобильных телефонов. Дистанционное банковское обслуживание требует комплексной защиты от фишинга и троянов для того, чтобы предотвратить изъятие конфиденциальной информации, хищение паролей.

Распространению киберпреступности в банковской сфере способствует использование банками устаревших технологий, не способных противостоять преступникам. Непростая экономическая ситуация в стране не подталкивает к значительному инвестированию банков в замену оборудования, установления современного высококачественного программного обеспечения. Банки вынуждены соизмерять степень риска и стоимость мероприятий по повышению уровня экономической безопасности. В свою очередь, отсутствует законодательный механизм ответственности производителей программного обеспечения перед своими клиентами. Предлагаемые продукты ПО в ряде случаев имеют слабую устойчивость к хакерским атакам и не соответствуют требованиям по безопасности.

Борьба с кибер-преступностью

В настоящее время действуют различные международные организации, деятельность которых направлена на борьбу с киберпреступностью.

Наиболее известным альянсом является Международное многостороннее партнерство против киберугроз (IMPACT), действующее как исполнительный орган в области кибербезопасности ООН. Эта организация объединяет усилия ряда государств, неправительственных организаций, экспертов в сфере информационной безопасности.

В 2011 г. был создан Международный альянс обеспечения кибербезопасности (ICSPA), объединивший правоохранительные органы, международный бизнес и правительства большинства стран мира.

Задача таких организаций состоит в выработке единых международных стандартов деяний, подлежащих криминализации, создании единой терминологии и понятийного аппарата, оказание консультационной помощи при принятии соответствующих уголовно-правовых норм на национальном уровне. Система сотрудничества, возникшая на базе Международной организации уголовной полиции, является достаточно развитой на данном историческом этапе. Она обеспечивает скорый и эффективный механизм сообщения между государством и Интерполом в осуществлении международного розыска и регистрации преступников. Несмотря на наличие существующих организаций и их активную деятельность, отсутствует

действительно эффективно налаженное международное сотрудничество спецслужб, в то же время у киберпреступников международная кооперация более совершенна и действенна.

Для комплексного противодействия киберпреступности необходимы:

– гармонизация уголовного законодательства о киберпреступности на международном уровне;

– разработка на международном уровне и имплементация в национальное законодательство процессуальных стандартов, позволяющих эффективно расследовать преступления в глобальных информационных сетях, получать, исследовать и представлять электронные доказательства с учетом трансграничности этих преступлений;

– отлаженное сотрудничество правоохранительных органов при расследовании киберпреступлений на оперативном уровне;

– механизм решения юридических вопросов в киберпространстве.

Кроме указанных мероприятий, на государственном и уровне частных предприятий необходимо активно заниматься профилактической, просветительской деятельностью.

Повышение компетенции в сфере компьютерных технологий отдельных пользователей, сотрудников компаний уменьшит риск стать жертвой киберпреступлений, снизит уровень «заболеваемости» информационных сетей.

Компьютерная грамотность населения позволит лучше понимать все угрозы, связанные с работой в социальных сетях, интернет-банкинге, при осуществлении онлайн-покупок.

Наконец, пользователям необходимо научиться быть менее беспечными, самим позаботиться о своей безопасности.

Интегративный и комплексный подходы в применении правоохранительными органами профилактических мер могут повысить уровень информационной безопасности России и сделать предупреждение компьютерных преступлений более эффективным. Предложенные превентивные меры дадут ощутимый результат только в случае совместных действий государства с институтами гражданского общества (органами местного самоуправления, образовательными и научными учреждениями, средствами массовой информации, общественными объединениями и т.д.)

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.

Список используемых источников

1. Номоконов В. А. Киберпреступность как новая криминальная угроза

2. Тарасов А. Электронный банкинг и его безопасность

3. ICT Facts and Figures – The world in 2015

4. Всемирный обзор экономических преступлений за 2016 год

5. Згадзай О. Э. Киберпреступность: факторы риска и проблемы борьбы

6. Чекунов И.Г. Киберпреступность: понятие, классификация, современные вызовы и угрозы

7. Рогозин В.Ю. Изменения в криминалистических характеристиках преступников в сфере высоких технологий

8. Тулегенов В.В. Киберпреступность как форма выражения криминального профессионализма

9. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение

10. Мороз Н.О. Деятельность Интерпола по координации сотрудничества в борьбе с преступностью в сфере высоких технологий

11. Журавленко Н.И. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере

12. Пархоменко С.В. Предупреждение компьютерной преступности в Российской федерации: интегративный и комплексный подходы / С.В. Пархоменко, К.Н. Евдокимов // Криминологический журнал Байкальского государственного университета экономики и права.