МОНГОЛ УЛС ДАХЬ КИБЕР ГЭМТ ХЭРГИЙН ӨНӨӨГИЙН БАЙДАЛ, ДҮГНЭЛТ, САНАЛ

СЕГОДНЯШНЕЕ СОСТОЯНИЕ КИБЕРПРЕСТУПЛЕНИИ В МОНГОЛИИ, ВЫВОДЫ И ПРЕДЛОЖЕНИЯ

NOWADAY SITUATION OF CYBER CRIME IN MONGOLIA, CONCLUSION AND PROPOSAL

Д.СУМЪЯАЦЭРЭН ХСИС-ийн Эрдэм шинжилгээ, хөгжлийн хүрээлэнгийн Цагдаа судлалын төвийн эрдэм шинжилгээний ажилтан, докторант, цагдаагийн ахлах дэслэгч

СУМЪЯАЦЭРЭН Д. Научный сотрудник центра полицейского исследования Института исследования и развития, Университета правоохранительного дела Монголии, докторант, старший лейтенант полиции

SUMIYATSEREN D. Researcher in Police studies center, Research and Development Institute, Law enforcement university, Police senior lieutenant

Товч агуулга: Тус өгүүлэлд Монгол Улс дахь кибер аюулгүй байдлын чиглэлээр идэвхтэй үйл ажиллагаа явуулдаг төрийн болон төрийн бус байгууллагуудын үйл ажиллагааны чиглэлийг тусгаж, Эрүүгийн хуулийн тусгай ангийн 25 дугаар бүлэг "Компьютер, мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг"-т зассан зүйл ангиар үүсгэсэн хэргийг сүүлийн 5 жилээр гаргаж, дүн шинжилгээ хийсэн болно. Мөн одоогийн хүчин төгөлдөр үйлчилж буй Эрүүгийн хууль болон шинээр боловсруулж буй Гэмт хэргийн тухай хуулийн төсөлд "Мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг" хэмээх бүлэг туссан байдлыг харьцуулан судалж, дүгнэлт, санал боловсруулав.

Аннотация: В статье рассматривается деятельности государственных и негосударственных организаций Монголии в сфере кибербезопасности. Анализировал статистику преступления рассмотрена в главе 25 особенной части Уголовного кодекса "Преступления против компьютерной и информационной безопасности" за последние 5 лет. Разработано сравнительное исследование УК Монголии и законопроект о преступлении, были разработаны выводы и предложения.

Abstract: In this article we are noting the activities of Governmental and Non-Governmental Organizations, which are conducting in the fields of Cyber crime and security in Mongolia, and also the monitoring on crime situation for last 5 years, mentioned at 25 article of Criminal Law of Mongolia "Crimes against computers and information security". The recommendation was represented comparing the valid variation of Criminal Law and new draft of Crime Law.

Общество, в котором мы живем и трудимся сегодня становится с каждым днем все более зависимым от потребления кибер оборудовании, таких, как компьютер, мобильные телефоны, таблеты и т.д.

В данный момент, когда интенсивное развитие информационной технологии является основной действующей силой экономики, общественной жизни, различного рода деятельностей в сферах обслуживания, услуг, предпринимательства и торговли, а также государственное обслуживание граждан страны осуществляется киберсистемой. Следовательно, проблема защиты общества от атак и нападения киберпреступности становится весьма актуальной.

В нашей стране впервые в 1961 году начал использовать компьютер под названием "Тайблятор", который был поставлен по заказу статистического управления Монголии и этот "Тайблятор" считается первым компьютером с программным управлениям, внедренным в Монголии. После этого, а именно в 1986 году были внедрены в использование персональные компьютеры, далее в 1994 году наша страна вошла в список стран мира, потребляющихся интернетом.

По исследованию Центра обслуживания общественной защиты установлено, что, хотя по сравнению с высокоразвитыми странами Монголия по качеству пользующихся интернетом контингента населения стоит на 102 месте из свыше 200

государств мира, но по процентному отношению ко всему населению занимает первое место в мире.

Государственные и негосударственные организации, осуществляющие активную деятельность по направлению кибербезопасности и основная направленность их деятельности

Руководитель национального центра Монголии по борьбе против кибератак и нападения, доктор Т.Халтар в интервью, данной газете "Өдрийн сонин" выразил свою точку зрения по этому вопросу следующим образом: "Повседневно в нашу страну поступают от 30 тысяч до 100 тысяч кибератак. Хотя около 80% этих кибератак и нападения составляют

№	Название организации	Направление деятельности
1	Совет национальной безопасности	Разработка комплексной политики информационной безопасности
2	Управление по кибербезопасности	- Обнаружение и выявление опасности кибератаки, засечение и оказание противодействия против неё в государственной обьединенной информационной коммуникационной сети; - Разработка документации, направленные на осуществление политики о кибербезопасности, выдача рисковой оценки, связанной с кибер и информационной безопасностью государственным организациям; - Организация обучения и рекламирования о кибербезопасности; - Создание и организация обьединенной сети государственных организации, а также системы специализированной государственной связи и засекреченной сети Главного разведывательного управления, несение ответственности за эксплуатацию оборудования и их реконструкционное обновление; - Обеспечение секретности и безопасности в процессе передачи и обмена государственных секретных информации между государственными и правительственными организациями.
3	Комитет по регулированию коммуникации и связи	- Защита прав потребителей, контроль и проверка, расследование, разбирательство жалоб, менежмент вебсайтов организации; - Специальное разрешение, стандартизация и утверждение, очередность, технические вопросы коммуникации,технические условия и требования, технологическая реконструкция, объединение и интернет; - Планировка радиочастот, технический анализ, распределение радиочастот и менежмент.
4	Управление по коммуникации и связи, почте и информационной технологии	- Внедрение современной техники и передовой технологии, почты, космической технологии, коммуникации и связи, осуществление программы реконструкции; - Создание благоприятной среды для развития кибер управления в Монголии, осуществление политики, стратегии и мер по данному направлению, обеспечение надежности и безопасности информации.
5	Национальный дата центр	- Обеспечение сохранения государственной кибердаты и информационной технологии в надлажащих условиях, охранности и доступности населению; - Обеспечение безопасности, сохранения, охранения государственной кибердаты и информации.
6	Национальный центр Монголии по борьбе против кибератак / MonCIRT/	Контроль за кибератак и выявление их.
7	Другие.	

.

попытки любителей хакеров внедряться в серверы каких – либо компании или организации, но остальное 20% вызывает особое опасение по причине того, что специально подготовленные высококвалифицированные лица скопируют информации без улик и каких нибудь след и такие кибератаки все более учащаются. Большинство кибер атак направляется ик Китая и России, далее следуют Тайвань, Южнай Корея, Япония, Бразилия и другие".

Что такое киберпреступление?

К киберпреступлениям относятся все виды преступных деяний, совершенные со использованием компьютеров, информационной сети и интернета. Киберпреступление делится на следующие виды:

- Против личности /вирус, мошенничество, фишинг, спэм и т.д./
- Против имущества /уничтожение имущества других лиц, распространение вредных программ и т.д./
- Против государства /кибертерроризм, информационная война/

Киберпреступление является понятием, охватывающим более широкий предель, чем определено санкциями 226 – 229 статей специального состава УК Монголии.

Хотя в основной концепции национальной безопасности Монголии особо определенно указана, что информационная безопасность является самостоятельным видам национальной безопасности , но до сих пор в нашей стране отсутствует базовый закон об информационной безопасности.

Киберпреступление против информационной безопасности и использования компьютеров /2006 – 2013/

Начиная с 2012 года на территории нашей страны выявлен ряд преступлении похищения крупных сумм денег со использованием фальшивых кредитных карт из автоматических машин для выдачи наличных денег коммерческих банков гражданами Украины и Малайзии. Было выявлено преступление, что граждане Малайзии использовав фальшивые кредитные карты коммерческих банков Монголии выкупили большую партию товаров в супермаркетах и крупных торговых центрах. Установлен тот факт, что они выкупив товары с отметкой "брэнд" и перевозив через государственную границу реализовали по более высоким ценам. При этом преступники хакерским способом внедрялись в чужие банковские счета и фальшивыми платежными картами расплачивались за покупки.

Установлено, что преступники похитили денежные средства в размере приблизительно 45 миллионов тугриков. Определено, что они изготовливают фальшивые банковские кредитные карты не только Монголии, но и других стран. Например, эти личности хакерским преступным способом крадут информации с черных лент банковских кредитных карт таких банков, как "Чейз", "Ай Ти Эс" и т.д. США и устанавливают на готовые матрицы, изготовленные в Малайзии. Таким образом, вся информация хозяина кредитной карты попадает в руки преступников.

Вообще, мировые массовые информационные средства время от времени сообщают о преступных группировках, специализирующихся в преступных деяниях, упомянутых выше. Поэтому международные банки постоянно улучшают и совершенствуют систему контроля, тем самым пресекают возможность мошенничества.

Тот факт, что последнее время эти преступные элементы стали в большом количестве внедряться в нашу страну, возможно связано с несовершенной контрольно – охранной системой коммерческих банков Монголии. Это свидетельствует о необходимости корренного улучшения охранной и контрольной системы банков.

Названное преступное деяние, или большинство киберпреступлении, совершенное в нашей стране рассматривается и осуждается до сих пор по статье 148 особенной части УК Монголии, как мошенничество, или присвоение чужих имуществ обманным путем. Это и есть свидетельство того, что из за несовершенной законо – правовой среды и отсутствия точной соответствующей санкции о борьбе против киберпреступности не имеется достаточное оснавание считать его преступлением. Например, в феврале 2013 года выявлена попытка внедрения извне во внутренную компьютерную сеть акционерной компании "Кашемир холдинг", которая находиться на территории района Хан-Уул города Уланбатора, и похитить денежные средства. Приостановленное и отказанное от возбуждения уголовное дело было возобновлено прокуратурой по п.4 ст.148 особенной части УК /присвоение чужих имуществ обманным путем/ и проверено.

Хотя редко, но граждане нашей страны становятся сообщником, или непосредственными исполнителями

кибер преступных деянии в зарубежных странах. В частности, в 2010 году выявлено преступление, что три гражданина Монголии многократным действием мошенничества присвоили крупную сумму денег со вкладов клиентов банка “Wells Fargo” ФРГ. А также в Индии двое наших граждан в сообществе хакерской группировки нанесло ущерб газете “Най Дунай” в размере 900 тысяч индийских рупи /около 17 тысяч американских долларов/.

Сравнение главы под названием “Преступление против информационной безопасности”, которая указана в действующем Уголовном кодексе с главой нового проекта закона о преступлении

№	Уголовный кодекс	В проекте
1	Ст.226 Изменить, испортить и уничтожить компьютерные информации 226.1. В случае преднамеренного изменения, нарушения, порчи компьютерной программы, компьютеров, их устройства, оборудования и информационную сеть подвергать денежную штрафу, превышающему минимальный размер заработной платы от 51 до 200 раза, или наложить арест от трех до шести месяцев, или назначить наказание заключения до двух лет в исправительных колониях.	Ст.26.1. Незаконная атака на серверы и киберинформации Если способам незаконной атаки на охраняемую информационную сеть уничтожены, изменены, испорчены, скопированы и добавлены информации, создания ситуации невозможности использовать программное обеспечение и информационную сеть, или нарушена их нормальная деятельность подвергать денежному штрафу от 7 до 36 милионов тугриков, или ограничить свободу на срок 1 до 5 лет, или назначить наказание в виде заключения от 1 до 5 лет в исправительных колониях.
	226.2. Если данное преступное деяние совершено в корыстных целях, а также по предварительной группой лиц, или со использованием служебных положении подвергать денежному штрафу, превышающему минимальный размер заработной платы от 100 до 250 раза, или назначить наказание в виде заключения от 3 до 5 лет в исправительных колониях.	
2	227. Приобретать компьютерные информации незаконным путем 227.1. если без разрешения соответствующих лиц скопировав сохраняющиеся и передающиеся информации в компьютерах и информационной сети, нанесли немалый ущерб другим лицам, или организациям подвергать денежную штрафу, превышаю щему минимальный размер заработной платы от 51 до 100 раза, или наложить арест от 3 до 6 месяцев, или наказание в виде заключения до двух лет в исправительных колониях.	26.2. Изготовление и реализация программ, технических средств и принадлежностей для незаконной атаки на серверы и киберинформации Если совершено преступное деяние изготовления и реализации специальной программы, или технических средств для незаконного внедрения в охраняемую информационную сеть и кибероборудование подвергать денежному штрафу в размере от 7 до 36 милионов тугриков , или ограничить свободу от одного до пяти лет содержать в заключении.
3	228. Изготовление и реализация специальных принадлажностей для незаконного внедрения в информационную сеть компьютеров 228.1. если изготовили и реализовали специальные программы, или технические средства для незаконного внедрения в компьютеры и охраняемую информационную сеть подвергать денежному штрафу, превышающему минимальный размер заработной платы от 51 до 150 раза, или наложить арест от 3 до 6 месяцев, или назначить наказание в виде заключения в исправительных колониях до 5 лет.	26.3. Если выявлено преступное деяние специальной разработки, использования и распространения вредного программного обеспечения для уничтожения, порчи, изменения, скопирования информации, хранящихся в кибер оборудованиях, серверах и нарушения их нормального функционирования следует подвергать денежному штрафу в размере от 7 до 36 милионов тугриков, или ограничить свободуют одного до пяти лет, или назначить наказание содержать в заключении сроком от одного до пяти лет.
	229. Разработка, использование и распространение с вирусам 229.1. Если выявлено преступное действие уничтожения без соответствующих разрешении информации, хранящихся в компьютерах, разработки программ с целью закрытия, изменения в программу, специальной разработки программы с вирусом и использования их следует подвергать денежному штрафу, превышающему минимальный размер заработной платы от 5 до 50 раза, или назначить принудительную работу сроком от 100 до 200 часов, или наложить арест до трех месяцев.	
	229.2. Если вследствие кибер преступного деяния нанесен крупный, или особо крупный ущерб другим лицам и организациям следует подвергать денежному штрафу, превышающему минимальный размер заработной платы от 51 до 250 раз, или наложить арест на срок от трех до шести месяцев, заключения до 5 лет в исправительных колониях.	

В 26.1 статье проекта закона “О преступлении” обьединили 226 и 227 статьи действующего УК в одну статью и все преступные действия незаконной атаки на охраняемую информационную сеть и кибер оборудование санкционированы считать преступлением. Все остальные статьи действующего УК по содержанию не претерпели существенных изменении.

Скаждымгодомувеличиваетсячислопотребителей вебсайтов социальной сети /Social network/. С тех пор, как в 2006 году был открыт фейсбук /facebook/, он получил широкое применение во всем мире. И в настоящее время 547 тысяч граждан нашей страны является потребителями данного сайта.

В последнее время участилось преступное деяние, что преступные личности, имеющие гражданства стран Азии, таких, как Филиппины, Сингапур, и Малайзии фальшивые аккаунты устанавливают связь с нашими гражданами, путем обмена информациями и видеочата собирают личные интимные и секретные информации граждан, а потом использовать их в незаконных сделках. Эти преступные личности добытые незаконным путем и скопированные видеозаписи устанавливает в вебсайты и угрожают, или шантажируют граждан тем, что их показать родным, близким, друзьям или другим лицам и требуют крупные суммы денег.

Сегоднящнее кибер состояние Монголии

- Недостаточно обустроенная законо – правовая среда.
- Малое количество квалифицированных специалистов по информационной безопасности.
- Хотя в Монголии имеется потенциальная возможность защиты и противодействия против кибератак, к сожалению, по направлению обеспечения информационной безопасности не осуществляется инвестрирование.
- Отсутствует обьединенная государственная внутренная информационная сеть.
- Государственные организации во внутренней сети используют беспроводную технологию.
- Хаотичный выход связи с интернетом.

Выводы и предложения

1. Важной проблемой борьбы против кибер преступления является в первую очередь создание благоприятной, соответствующей законо – правовой среды, подготовка высоко квалифицированных кадров /специалистов/, а также обеспечение надлежащими техническими средствами и оборудованиями.
2. Появилась необходимость комплексного решения вопроса об информационной безопасности путем принятия закона об информационной безопасности и её охране. По этому в главном управлении разведки создана рабочая комиссия по разработке проектов общих законов об обеспечении информационной безопасности и о кибер безопасности.
3. По этому направлению США и Южная Корея занимают главенствующий роль в мире. По этому необходимо в сотрудничестве с Южной Корей осуществлять программу по исследованию проблемы о борьбе против киберпреступления, либо кибер – следователей, создать лабораторию по исследованию и анализу данного вида преступлений.
4. Киберпреступление не имеет границ. По скольку для выявления этого вида преступлении весьма важно международное совместное сотрудничество нашей стране следует как можно скорее присоединиться в Будапештскую конвенцию по борьбе против киберпреступлении, которая была принята в 2001 году.