УДК 351.865

Гуменяк Д.В., Москаленко В.И., Никулищев Г.И.
Запорожский национальный технический университет

Современные подразделения кибербезопасности Украины

В наши дни большинство людей значительную часть своего времени проводят в Интернете. Этот виртуальный мир во многом отражает мир реальный: преступность, являющаяся, к сожалению, неотъемлемой частью социума, существует и в виртуальном мире. Под киберпреступностью понимается совокупность преступлений, совершаемых в киберпространстве с помощью и против компьютерных систем или компьютерных сетей. Растущий обмен информацией в Интернете и электронные платежи - это именно тот лакомый кусок, который более всего привлекает злоумышленников.

В сложной социальной и политической обстановке современной Украины борьба с киберпреступностью и обеспечение кибербезопасности являются задачами повышенной актуальности. Решением данных задач занимаются профильные спецподразделения государственных силовых ведомств. В работе рассматриваются цели и задачи подразделений, а также производится сравнение их полномочий, возможностей и компетенций.

Для борьбы с киберпреступностью, постановлением Кабинета Министров Украины от 13 октября 2015 года было принято решение "Об образовании в качестве юридического лица публичного права Департамента киберполиции как межрегионального территориального органа Национальной полиции".

Цель создания - реформирование и развитие подразделений МВД Украины, что должно обеспечить подготовку и функционирование высококвалифицированных специалистов в экспертных, оперативных и следственных подразделениях полиции, задействованных в противодействии киберпреступности.

Основные задачи киберполиции.

1. Реализация государственной политики в сфере противодействия киберпреступности.

Противодействие киберпреступлениям:

- в сфере использования платежных систем;
- в сфере электронной коммерции и хозяйственной деятельности;
- в сфере информационной безопасности.

2. Заблаговременное информирование населения о появлении новейших киберпреступлений.

3. Внедрение программных средств для систематизации и анализа информации о киберинцидентах, киберугрозах и киберпреступлениях.

4. Реагирование на запросы зарубежных партнеров, которые будут поступать по каналам Национальной круглосуточной сети контактных пунктов.

5. Участие в международных операциях и сотрудничество в режиме реального времени. Обеспечение деятельности сети контактных пунктов между 90 странами мира.

В Украине также функционирует специализированное структурное подразделение Государственного центра киберзащиты и противодействия киберугрозам – CERT-UA.

Основная цель CERT-UA – обеспечить защиту государственных информационных ресурсов, информационных и телекоммуникационных систем от несанкционированного доступа, неправомерного использования и нарушения их конфиденциальности, целостности и доступности.

Функциональные направления деятельности CERT-UA:

1. Предупреждение и предотвращение реализации киберугроз.

2. Мониторинг и обнаружение киберугроз.
3. Изучение и анализ компьютерных инцидентов.
4. Расследование и ликвидация киберугроз.

Среди основных угроз, противодействием которым занимается CERT-UA: вредоносное ПО, ботнеты, интернет-мошенничество, DDos-атаки, эксплуатация уязвимостей в программном и аппаратном обеспечении, несанкционированный доступ к автоматизированным/информационным системам, веб-ресурсам и нарушение штатного режима их функционирования.

Законом Украины от 7 сентября 2005 года № 2824-IV была ратифицирована Конвенция о киберпреступности. В части первой второго раздела установлены мероприятия по кибербезопасности, проводимые подразделениями на национальном уровне. На основе данной конвенции авторами была проведена сравнительная характеристика двух подразделений, которые выполняют предписанные мероприятия.

Таблица 1 – Сравнительная характеристика подразделений киберполиции и CERT-UA

Предотвращаемые угрозы	Киберполиция	CERT-UA
Незаконный доступ	+	+
Нелегальный перехват	+	+
Вмешательство в данные	+	+
Вмешательство в систему	+	+
Злоупотребления устройствами	+	-
Подделка, связанная с компьютерами	+	-
Мошенничество, связанное с компьютерами	+	+/-
Правонарушенния, связанные с детской порнографией	+	-
Правонарушенния, связанные с нарушением авторских и смежных прав	+	-
Санкции и меры	+/-	-

Результаты сравнения, представленные в таблице 1, позволяют сделать вывод, что подразделение CERT занимается кибербезопасностью государственных структур, обеспечивая постоянный мониторинг системы и обнаружение угроз. А киберполиция – борется непосредственно с киберпреступностью, наделена соответствующими правами, а также заблаговременно информирует население об опасности и поддерживает сотрудничество с зарубежными партнерами.

Между тем, любой гражданин, при обнаружении киберпреступления или попытке его совершить, может обратиться, как и в киберполицию, так и CERT. Данные подразделения тесно сотрудничают между собой и имеют общие задачи для решения, такие как предотвращения и ликвидация киберугроз.

Список использованной литературы

1. *Официальный портал верховной Рады Украины: постановление Кабинета Министров Украины от 13 октября 2015 года "Об образовании как юридическое лицо публичного права Департамент киберполиции как межрегиональный территориальный орган Национальной полиции" [Електронний ресурс]: Верховная Рада Украины. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/831-2015-%D0.*
2. *Официальный портал верховной Рады Украины: конвенция про киберпреступность [Електронний ресурс]: Верховная Рада Украины. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/994_575/page.*
3. *Официальный сайт CERT-UA: [Електронний ресурс]: Computer Emergency Response Team of Ukraine. – Режим доступу: http://cert.gov.ua/.*