Комитет №12

Кибербезопасность

Доклад эксперта

ФОРУМ ПО УСТОЙЧИВОМУ РАЗВИТИЮ

КИБЕРБЕЗОПАСТНОСТЬ
Комитет №12

Кибербезопасность в системе международных отношений

Переступая порог информационной эпохи, мы сталкиваемся как с новыми возможностями, так и с новыми угрозами. С развитием информационно-коммуникационных технологий проблема кибербезопасности выходит на передний план. Повсеместная цифровизация ставит под угрозу все сферы общества.

Кибербезопасность – это реализация мер по защите систем, сетей и программных приложений от цифровых атак, которые обычно направлены на получение доступа к персональной информации, на ее изменение и уничтожение, на вымогательство у пользователей денег или на нарушение нормальной работы компаний. Реализация мер эффективной кибербезопасности сегодня становится достаточно сложной задачей, так как сегодня имеется гораздо больше устройств, чем людей, а злоумышленники становятся все более изобретательными. Почти 50 лет назад был написан первый вирус-червь «Creeper». Он не был полноценным вирусом, поскольку не причинял никакого вреда системе. Вместо этого он искал по сети компьютеры, самостоятельно копировался и выводил на терминале специфичное сообщение. Сейчас же киберугрозы шагнули далеко вперёд, причиной этому стало развитие глобальной сети. Если появляется возможность заработать, появляются и те, кто этим пользуется. Так начали развиваться различные программы для вымогательства или кражи конфиденциальной информации, а также для парализации работы различных систем. Появилось malicious software или сокращённо malware. Malware – это любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самого компьютера или к информации, хранимой на жёстком диске компьютера с целью использования ресурсов или причинения вреда владельцу информации, компьютера или владельцу сети путём ее копирования, искажения, удаления или подмены. Одним их Самых распространённых типов вредоносных программой является «Trojan horse». Trojan horse – это вирус, названный в честь известного мифа о троянском коне. Данный вирус побуждает пользователя запустить программу и после запуска происходит инфицирование устройства. После этого, в зависимости от цели, вирус начинает шпионить за пользователем, получает контроль над компьютером или полностью блокирует систему, требуя денежного вознаграждения. Лица, которые совершают кибератаку, называются «hacker» или «cracker». Наиболее популярный, но не совсем верный термин, это хакер. Хакеры бывают как «black hat», так и «white hat»: соответственно те, кто совершают взлом с целью получения личной выгоды и те, кто предотвращает атаки и «залатывает дыры» в системе безопасности. На данный момент киберпространство плохо регулируется или не регулируется вовсе и представляет собой своеобразную «киберанархию». В сети распространён интернет буллинг, фишинг, вымогательства и т.д. Достаточно сложно или невозможно определить преступника. Таким же образом в Darknet работают группы хакеров, занимающиеся кражей конфиденциальной информации, финансов. Не регулируемая часть интернета, так называемая «Darknet», это скрытая сеть, соединения в которой устанавливаются только между доверенными «пирами» (равноправными участниками сети), иногда именующимися как

«друзья», с использованием нестандартных протоколов и портов. Огромнейшую опасность несут в себе кибератаки на промышленность или государственные структуры. Такие атаки помимо финансового ущерба, могут привести к катастрофам с человеческими жертвами. Поэтому одной из важнейших задач является внесение интернет пространства в правовое поле для своевременной идентификации преступников и предупреждения правонарушений. Стоит отметить, что уязвимостью в кибербезопасности пользуются не только неправительственные организации, но и сами правительства ряда стран. Так, 12 государств официально объявили о создании специальных подразделений, призванных осуществлять не только кибероборону, но и кибератаки. Появляется новое явление называемое «Cyberwarfare» или кибервойна. Кибервойна – это военные действия, осуществляемые электронным способом, где в качестве оружия используется информация, а инструментами выступают компьютеры и интернет. Она является одной из разновидностей информационной войны и представляет собой противостояние в кибернетическом пространстве. Приоритетом кибервойны является не только нанесение ущерба противнику, но и защита собственных данных, поэтому кибербезопасность – неотъемлемая часть противостояния. Целью кибервойны является дестабилизация режима в государстве, парализация работы государственных сайтов, выведение из строя промышленных объектов, а также кража секретной информации. По статистике компании «АМТ-Груп» главной целью является топливно-энергетический комплекс. Одним из примеров кибератаки является атака на Бушерскую АЭС в Иране. Она была проведена сетевым червём Stuxnet, который поразил центрифуги по обогащению урана. Вероятными агрессорами выступили США и Израиль, которые написали данный вирус. Стоит отметить, что компьютеры на АЭС были изолированы от глобальной сети и для инфицирования потребовался работник, который вероятно пронёс вирус на USB -flash-накопителе. Другой серьезной угрозой международной кибербезопасности является кибертерроризм. Кибертерроризм – это комплекс незаконных действий, создающих угрозу государству и обществу. Официально кибертерроризм - это акты, которые совершаются как и одним человеком, так и группировкой. Если в кибертерроризме принимает участие представители правительственных или иных государственных структур, это считается проявлениями кибервойны. Объектами могут являться государства, международные организации, крупные и относительно небольшие компании, политические деятели, а также выбранные случайным образом люди. Действия кибертеррористов могут быть направлены на объекты гражданской инфраструктуры и военного назначения. Развитие технологий позволит решить некоторые проблемы, связанные с уязвимостями в глобальной системе кибербезопасности. Так, квантовые технологии позволят обезопасить конфиденциальные данные пользователей через шифрование в режиме «одноразовых блокнотов». Развитие искусственного интеллекта поможет обнаружить слабые места в системе безопасности. Однако новые технологии предоставляют больше возможностей злоумышленникам. По данным Juniper Research в 2018 году урон компаний от хакерских атак составил 3 триллиона долларов. Эксперты говорят о том, что киберпреступники сегодня используют все более ухищренный методы и инструменты, такие как искусственный интеллект, изучающий поведение систем безопасности и подобный тому, который используются ИБ-компании для обнаружения аномальной активности в ИТ-инфраструктуре. Кроме того, специалисты предупреждают о росте киберпреступности в социальных сетях и развитии таких технологий, как «deepfake», которые с помощью ИИ позволяют создавать «фейковые»

видеоролики с подменой лиц у действующих героев. В Juniper Research считают, что потери бизнеса от кибератак и последовавших от них утечек данных будут расти и превысят $5 трлн. Огромным шагом является выход проблемы кибербезопасности на международный уровень. Была принята резолюция Генеральной Ассамблеи ООН 57/239 «Создание глобальной культуры кибербезопасности» от 2002 года, а также резолюция Генеральной Ассамблеи ООН 72/200 « Использование информационно-коммуникационных технологий в целях устойчивого развития» от 2017 года. Каждый член общества должен иметь равный доступ к информации, а также защиту от угроз, исходящих из киберпространства. Большим шагом в построение системы кибербезопасности в рамках НАТО является создание «Таллинского руководства по международному праву, применимому к кибервойнам» от 2013 года, а также второе издание данного руководства от 2017 года. Серьёзный вклад в обеспечение кибербезопасности вносит ОБСЕ: решение №1202 призывает государств-членов к координированной работе в сфере обнаружения угроз, исходящих из киберпространства. Наибольших успехов в области кибербезопасности добился Европейский Союз. Например, в 2016 году им была принята директива о безопасности сетевых и информационных систем. Она обязательна для исполнения и образует систему, предупреждающую киберугрозы на территории ЕС, а также способствует расширению правового поля ЕС на киберпространство. Таким образом, следует стремиться к усилению роли государственных и международных институтов для регулирования киберпространства с учетом прав и свобод граждан.

ИСТОЧНИКИ

1. https://www.itu.int/dms_pub/itu-d/opb/stg/D-STG-SG01.22-2010-PDF-R.pdf
2. https://undocs.org/ru/A/RES/2844%28XXVI%29
3. https://www.un.org/ru/documents/decl_conv/conventions/elements.shtml
4. https://interaffairs.ru/jauthor/material/1718
5. https://interaffairs.ru/jauthor/material/1718
6. https://www.imemo.ru/files/File/ru/publ/2016/2016_037.pdf
7. https://postnauka.ru/longreads/82777
8. https://postnauka.ru/video/83002
9. https://postnauka.ru/video/82831

Бразилия

1. https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf
2. https://www.researchgate.net/publication/329973217_A_Strategy_for_Cybersecurity_Governance_in_Brazil
3. https://brazilian.report/power/2019/07/25/brazil-handle-cyber-security-issues/
4. https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=37581&sid=128#.XdrdS5MzaUk
5. https://www.trendmicro.com.ru/cloud-content/us/pdfs/security-intelligence/white-papers/wp-brazil.pdf

Великобритания

1. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
2. https://www.ncsc.gov.uk/
3. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf
4. https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/1745/1745.pdf

Греция

1. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view
2. https://www.cyberwiser.eu/greece-gr
3. https://cybersecuritymonth.eu/ecsm-countries/greece
4. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/greece
5. http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_greece.pdf

Иран

1. https://russiancouncil.ru/cyberiran
2. https://www.csis.org/analysis/iran-and-cyber-power
3. http://www.iimes.ru/?p=40770
4. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CSIS%20-%20Cybersecurity%20and%20Stability%20in%20the%20Gulf.pdf
5. https://www.cybersecurity-insiders.com/iran-cyber-attacks-the-uk/

Канада

1. https://www.cyber.gc.ca/en
2. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx
3. https://www.canada.ca/en/services/defence/cybersecurity.html
4. https://www.cse-cst.gc.ca/en/backgrounder-fiche-information
5. https://www.ic.gc.ca/eic/site/137.nsf/eng/home

Конго

1. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/congo-r
2. https://cd.usembassy.gov/u-s-drc-host-central-african-cybersecurity-cybercrime-workshop-kinshasa/
3. https://blogs.letemps.ch/solange-ghernaouti/2018/09/19/souverainete-numerique-et-dematerialisation-au-congo-brazzaville/
4. https://congodigital.net/index.php/tag/cybersecurite/

Корейская Народно-Демократическая Республика

1. https://www.csis.org/analysis/north-korea%E2%80%99s-cyber-operations
2. https://russiancouncil.ru/en/cybernorthkorea
3. https://www.scmp.com/week-asia/geopolitics/article/2187363/north-korean-cyberwarfare-big-threat-its-nuclear-weapons
4. https://www.researchgate.net/publication/325869138_Cyber_disruption_and_cybercrime_Democratic_People's_Republic_of_Korea
5. https://georgetownsecuritystudiesreview.org/2018/04/22/dprk-cyber-capabilities/

Мадагаскар

1. https://www.unodc.org/e4j/data/_university_uni_/cybersecurity_capacity_review_of_the_republic_of_madagascar.html?lng=en&match=Cybersecurity%20Capacity%20Review%20of%20the%20Republic%20of%20Madagascar
2. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/madagascar
3. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Madagascar.pdf
4. http://africapolicyreview.com/the-challenge-of-building-cyber-security-capability-in-africa/
5. http://www.artec.mg/pdf/cmm_rapport_final_cybersecurite_madagascar.pdf

Норвегия

1. https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf
2. https://www.regjeringen.no/en/dokumenter/national-cyber-security-strategy-for-norway/id2627177/
3. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/norway
4. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategy-for-information-security
5. https://www.cyberwiser.eu/norway-no

Россия

1. http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf
2. http://federalbook.ru/files/BEZOPASNOST/soderghanie/NB%20I/IX/Gattarov.pdf
3. https://studyinrussia.ru/en/study-in-russia/programs/30820-cybersecurity/description/
4. https://www.pwc.ru/ru/services/audit/riskassurance/cyber-security.html
5. https://www.cybersecurity-review.com/tag/russia/

США

1. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
2. https://www.dhs.gov/topic/cybersecurity
3. https://www.us-cert.gov/
4. https://www.us-cert.gov/nccic
5. https://www.cisa.gov/

Украина

1. https://gettingthedealthrough.com/area/72/jurisdiction/63/cybersecurity-ukraine/
2. https://www.researchgate.net/publication/321037340_The_System_of_Cybersecurity_in_Ukraine_Principles_Actors_Challenges_Accomplishments
3. https://ccdcoe.org/uploads/2018/10/NationalCyberSecurityStrategy_Ukraine.pdf
4. https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&ved=2ahUKEwi9gLKs4YzmAhWKE5oKHWynD9AQFjAIegQIAxAC&url=https%3A%2F%2Fdefense-reforms.in.ua%2Fen%2Fdownload%3Fpath%3D%252Ffiles%252FPress%252FGeneral%252FInfographics%252FSD_EN_Cyber_Strategy.pdf&usg=AOvVaw2R3PoXLD_IztkozJDKOpe2
5. https://delo.ua/special/sostojanie-kiberbezopasnosti-v-ukraine-nezavisimaja-vneshnjaja-o-346292/
6. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/ukraine

Франция

1. https://www.ssi.gouv.fr/publication/la-strategie-de-la-france-en-matiere-de-cyberdefense-et-cybersecurite/
2. https://www.itgovernance.eu/fr-fr/qu-est-ce-que-la-cybersecurite-fr

3. https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/
4. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/information-systems-defence-and-security-frances-strategy
5. https://www.ssi.gouv.fr/en/cybersecurity-in-france/

Швейцария

1. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategy-for-switzerlandss-protection-against-cyber-risks
2. https://www.cyberwiser.eu/switzerland-ch
3. https://www.s-ge.com/en/publication/fact-sheet/cybersecurity-switzerland
4. https://swiss-cybersecurity.ch/
5. https://gettingthedealthrough.com/area/72/jurisdiction/29/cybersecurity-switzerland/

Япония

1. https://www.j-cic.com/en/
2. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/japan
3. https://theowp.org/japans-cybersecurity-initiative/
4. https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-shousaigaiyou-en.pdf
5. https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf