Семинар 3

Международная информационная безопасность

Международная информационная безопасность

Международная информационная безопасность — состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве;

Информационное пространство - сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию;

(Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, Екатеринбург, 16 июня 2009 года)

Международная информационная безопасность

ДЕСЯТЫЙ МЕЖДУНАРОДНЫЙ ФОРУМ

«Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»

Сроки проведения: 25 - 28 апреля 2016 года.
Место проведения: Гармиш-Партенкирхен, г.Мюнхен, Германия.

Цели проведения Десятого Форума: выявление общих подходов и позиций экспертного сообщества по следующим актуальным проблемам международной информационной безопасности:

1. **Предложения в проект Кодекса ответственного поведения государств в информационном пространстве.**
2. **Толкование основных понятий, принципов и норм Женевских конвенций применительно к киберпространству.**
3. **Механизмы и инструменты частно-государственного партнерства в области обеспечения информационной безопасности критически важных объектов.**
4. **Меры противодействия Интернет-рекрутингу и Интернет-пропаганде экстремизма и терроризма.**
5. **Проблемы нераспространения кибероружия и уменьшения опасности его использования.**

Предложения в проект Кодекса ответственного поведения государств в информационном пространстве.

30.06.1520:19

Об итогах заключительного заседания Группы правительственных экспертов ООН по международной информационной безопасности.

Группа подтвердила суверенное право государств распоряжаться информационно-коммуникационной инфраструктурой на своей территории и определять свою политику в сфере международной информационной безопасности (МИБ).

Новым элементом доклада Группы стало положение о том, что любые обвинения государств в организации и совершении противоправных деяний с использованием ИКТ должны быть доказаны.

В докладе признается, что международное право применимо к сфере использования ИКТ, однако, в случае необходимости, оно может быть развито, в том числе за счет принятия новых принципов и норм. В этом контексте особое внимание уделено вопросу выработки норм, правил и принципов ответственного поведения государств в информационном пространстве.

Доклад Генеральному секретарю ООН для представления на 70-й сессии Генеральной Ассамблеи ООН.

Подпункт a) «в соответствии с целями Устава ОрганизацииОбъединенных Наций, в том числе касающимися поддержания международного мира и безопасности, государства должны сотрудничать в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ и предупреждению совершения действий в сфере ИКТ, признанных вредоносными или способных создать угрозу международному миру и безопасности»

Подпункт b) «в случае инцидентов в сфере ИКТ государства должны изучить всю соответствующую информацию, в том числе более общий контекст события, проблемы присвоения ответственности в ИКТ-среде, а также характер и масштабы последствий»

Доклад Генеральному секретарю ООН для представления на 70-й сессии Генеральной Ассамблеи ООН.

Подпункт c) «государства не должны заведомо позволять использовать их территорию для совершения международно-противоправных деяний с использованием ИКТ»

Подпункт d) «государства должны рассмотреть вопрос о наилучших путях сотрудничества в целях обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ, а также осуществлять другие совместные меры по противодействию таким угрозам. Государствам, возможно, потребуется рассмотреть вопрос о разработке новых мер в этой сфере»

Доклад Генеральному секретарю ООН для представления на 70-й сессии Генеральной Ассамблеи ООН.

Подпункт e) «в процессе обеспечения безопасного использования ИКТ государства должны соблюдать положения резолюций 20/8 и 26/13 Совета по правам человека о поощрении, защите и осуществлении прав человека в Интернете и резолюций 68/167 и 69/166 Генеральной Ассамблеи о праве на неприкосновенность личной жизни в эпоху цифровых технологий, чтобы обеспечить всестороннее уважение прав человека, включая право свободно выражать свое мнение»

Толкование основных понятий, принципов и норм Женевских конвенций применительно к киберпространству

Проблемные вопросы:

- Суверинитет в киберпространстве.
- Лимитация границ.
- Атрибуция инцидентов.
- Фрагментация интернета — аспекты:
  - Технические
  - Военные (красная кнопка)
  - Государственные
  - Экономические

Толкование основных понятий, принципов и норм Женевских конвенций применительно к киберпространству

Части международного права вооруженных конфликтов:

• право применения силы (Jus ad Bellum), определяющее условия, при которых сила может быть применена государством в международных отношениях, включая обеспечение самообороны; (ст. 41 и 42 Устава ООН, выделяют два основных вида «силы» — сила, связанная с использованием вооруженных сил (оружия) и сила, не связанная с использованием оружия).

• право ведения войны (Jus in Bello), определяющее правила применения государством и негосударственными образованиями вооруженной силы в процессе международных и немеждународных конфликтов, в том числе соблюдения ограничений гуманитарного характера. (Гаагские конвенции, Женевские конвенции и другие международные договоры, подписанные в развитие норм и идей данных конвенций, которые регулируют отношения, связанные с уменьшением физических страданий лиц, непосредственно затронутых военными действиями, ущерба имуществу гражданского населения, а также с обеспечением сохранности культурных ценностей).

Доклад Генеральному секретарю ООН для представления на 70-й сессии Генеральной Ассамблеи ООН.

Подпункт i) «государства должны принимать разумные меры для обеспечения целостности каналов поставки, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ. Государства должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование пагубных скрытых функций»

Подпункт j) «государства должны способствовать ответственному представлению информации о факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости, чтобы ограничить, а по возможности и устранить возможные угрозы для ИКТ и зависящей от ИКТ инфраструктуры»

Доклад Генеральному секретарю ООН для представления на 70-й сессии Генеральной Ассамблеи ООН.

Подпункт k) «государства не должны осуществлять или заведомо поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренной готовности к компьютерным и инцидентам (также именуемым группами готовности к компьютерным инцидентам или группам готовности к инцидентам в сфере кибербезопасности) другого государства. Государство не должно использовать уполномоченные группы экстренной готовности к компьютерным инцидентам для осуществления злонамеренной международной деятельности»

Доклад Генеральному секретарю ООН для представления на 70-й сессии Генеральной Ассамблеи ООН.

Подпункт k) «государства не должны осуществлять или заведомо поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренной готовности к компьютерным и инцидентам (также именуемым группами готовности к компьютерным инцидентам или группам готовности к инцидентам в сфере кибербезопасности) другого государства. Государство не должно использовать уполномоченные группы экстренной готовности к компьютерным инцидентам для осуществления злонамеренной международной деятельности»

Толкование основных понятий, принципов и норм Женевских конвенций применительно к киберпространству

Проблемы нераспространения кибероружия и уменьшения опасности его использования.

Проблемные вопросы:

- Кибероружие, Киберконфликт, Кибервойна.
- Опознавание объетов защищаемых МГП.
- Комбатанты, признаки комбатантов.
- Критическиважные объекты инфраструктуры.

ИЗВЕСТНЫЕ ИНЦИДЕНТЫ НА ЯДЕРНЫХ ОБЪЕКТАХ

(Алексей Лукацкий «КИБЕРБЕЗОПАСНОСТЬ ЯДЕРНЫХ ОБЪЕКТОВ» http://www.pircenter.org/media/content/files/13/14513827960.pdf)

- АЭС Sellafield, Великобритания, 1991 г.;
- Игналинская АЭС, Литва, 1992 г.;
- АЭС Бредвелл, Великобритания, 1999 г.;
- АЭС David Besse, США, 2003 г.;
- АЭС, Япония, 2005 г.;
- АЭС Browns Ferry, США, 2006 г.;
- АЭС Hatch, США, 2008 г.;
- АЭС в Майами, США, 2008 г.;
- АЭС Areva, Франция, 2011 г.;
- АЭС San Onofre, США, 2012 г.;
- АЭС Susquehanna, США, 2012 г.;
- АЭС Monju, Япония, 2014 г.;
- АЭС KHNP, Южная Корея, 2014 г..

ИЗВЕСТНЫЕ ИНЦИДЕНТЫ НА ЯДЕРНЫХ ОБЪЕКТАХ

Самая последняя из известных атак на атомный объект южнокорей ской корпорации KHNP (занимает 5-е место в мире по выработке атомной энерии) произошла в декабре 2014 г. В рамках данной атаки пока не установленные (или публично не названные) злоумышленники направили партнерам и бывшим сотрудникам АЭС по электронной почте письмо, содержащее вредоносный код.

Открытие данного письма привело к заражению компьютера и утечке данных, касающихся ядерных объектов KHNP. Второй стадией атаки стал взлом веб-сайта, на котором располагалось сообщество бывших сотрудников KHNP. В результате использования украденной учетной записи бывшего сотрудника была добыта очередная порция материалов, касающихся частной жизни действующих сотрудников корпорации KHNP. Наконец, на третьей стадии злоумышленники, воспользовавшись полученными сведениями, направили действующим сотрудникам атомных объектов KHNP специально подготовленные письма, которые должны были вызвать доверие и тем самым повысить шансы на успешное заражение компьютеров во внутренней сети KHNP.

ИЗВЕСТНЫЕ ИНЦИДЕНТЫ НА ЯДЕРНЫХ ОБЪЕКТАХ

Второй пример, это инцидент, произошедший в 2003 г. на атомной электростанции David Besse в Огайо (США). Внутренняя сеть компании, обслуживающей АЭС в Огайо, была заражена червем Slammer, который заражал сервера с программным обеспечением MS SQL Server 2000. В процессе проведения регламентных работ и в нарушение всех установленных на АЭС политик безопасности сотрудник обслуживающей организации установил прямое соединение между АЭС и сетью своей компании, чем не преминул воспользоваться вредоносный код, попавший внутрь сети АЭС David Besse. Неконтролируемое распространение червя привело к перегрузке сети и невозможности компьютеров в ней общаться друг с другом. В итоге система отображения параметров безопасности (SPDS) была недоступна в течение 6 часов 9 минут.

ИЗВЕСТНЫЕ ИНЦИДЕНТЫ НА ЯДЕРНЫХ ОБЪЕКТАХ

Инцидент произошел во Флориде в 2008 г. Инженер, обслуживающий обычную электростанцию в западном Майами, в обход всех правил отключил основную и резервную системы противоаварийной защиты. В результате последующего сбоя из строя было выведено оборудование подстанции, а система противоаварийной автоматики не смогла его предотвратить. В итоге пострадало свыше 680 тыс. потребителей, оставшихся без электричества. Несколько компаний, продающих электроэнергию, потеряли контроль над своими энергосетями. В том числе пострадала атомная станция Turkey Point на юге Майами.

А в 1992 г. в Литве, программист Игналинской АЭС загрузил вредоносный код в автоматизированную систему, отвечающую за работу одной из подсистем реактора. Данный факт был своевременно обнаружен, для проведения всестороннего расследования АЭС была остановлена. Аналогичная ситуация, когда внутренний нарушитель действовал со злым умыслом, произошла в 1999 г. на АЭС в Бредвелле (Великобритания). В инциденте участвовал сотрудник службы безопасности атомной электростанции.