4. Космический уборщик: робот очистит орбиту Земли от мусора – URL: https://www.techinsider.ru/science/news-373572-kosmicheskiy-uborshchik-robot-ochistit-orbitu-zemli-ot-musora/ (дата обращения: 14.04.2022). – Текст: электронный.

Черкасова Надежда Дмитриевна, магистрант гр.140101б, nady-cherkasova@yandex.ru, Россия, Тула, Тульский государственный университет.

ECO-ROBOTS IN MODERN WORLD

N.D. Cherkasova

A brief overview of robotic systems that are used to solve environmental problems (garbage sorting, cleaning water bodies, land and even outer space from waste) is presented. Examples of robots are also given that help in the settlement of emergency situations – environmental disasters (oil spills).

Keywords: environmental robots, waste sorting, cleaning robot, smart urn, robot.

Cherkasova Nadezhda Dmitrievna, student, nady-cherkasova@yandex.ru, Russia, Tula, Tula State University.

УДК 004.056.5

АНАЛИЗ ПРОЦЕССОВ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Совгирь А.В., Чернов Д.В.

В настоящей статье рассмотрены наиболее распространенные инциденты информационной безопасности киберпространства в контексте соответствия модели проникновения потенциального нарушителя режима информационной безопасности в информационную систему. Авторами представлено описание этапов процесса реагирования на инциденты информационной безопасности.

Ключевые слова: информационная безопасность, инцидент, Kill Chain, управление инцидентами.

В современном мире, для повышения эффективности своей деятельности, промышленные организации все больше создают информационные системы, информационно–телекоммуникационные сети и автоматизированные системы управления, предназначенные для автоматизации управленческих, технологических, экономических и (или) иных процессов. Ввиду увеличения их числа растёт и количество инцидентов информационной безопасности (далее ИБ). Одной из главных задач специалистов по защите информации является осуществление

процессов управления информационной безопасности в постоянно меняющемся ландшафте угроз киберпространства.

Цель работы заключается в анализе предметной области обеспечения процессов управления инцидентами ИБ, существующей отечественной нормативно-методической базе, посвященной процессам управления инцидентами ИБ, а также сопоставлении вышеуказанных процессов лучшим мировым практикам обеспечения ИБ.

Согласно положениям государственного стандарта [1], инцидент ИБ – это одно или несколько нежелательных или неожиданных событий информационной безопасности, которые с высокой степенью вероятности могут привести к компрометации в бизнес–процессах и создают угрозы для информационной безопасности. Выделяют четыре распространённых типа инцидентов информационной безопасности [2]:

- DDoS – атака это попытка злоумышленника перенаправить трафик на целевое приложение или интернет–приложение, бомбардируя их большим количеством запросов;
- Вредоносное программное обеспечение (далее вредоносное ПО) - программное обеспечение, созданное для повреждения, нарушения работы или получения незаконного доступа к клиенту, компьютеру, серверу или компьютерной сети. Программа–вымогатель, разновидность вредоносного ПО, угрожает уничтожить или скрыть данные или файлы жертвы, если не будет выплачен выкуп за расшифровку и восстановление доступа;
- Фишинг - мошенническая попытка, обычно по электронной почте, получить конфиденциальную информацию, выдавая себя за авторитетное юридическое или физическое лицо. Он использует человеческие эмоции, чтобы создать ощущение срочности и вызвать реакцию. Поскольку фишинг широко распространен в рабочей среде, он представляет собой постоянную угрозу и занимает первое место в рейтинге IBM X–Force Threat Intelligence Index 2020 [3];
- Внутренние угрозы исходят от пользователей, которые имеют авторизованный и законный доступ к активам компании и намеренно или случайно злоупотребляют ими. Внутренние нарушители зачастую знают местоположение конфиденциальных данных организации, и имеют повышенный уровень доступа, независимо от того, имеют ли они злонамеренные намерения или нет.

По результатам проведенного анализа ежегодных отчетов ведущих компаний – производителей средств защиты информации, зафиксировано возрастающее число инцидентов, являющихся частью модели Kill Chain.

Модель Kill Chain представляет собой цепи последовательных действий киберпреступника, направленных на взлом инфраструктуры и компрометацию ключевых ресурсов компании [3,4,5]. Концепция модели Kill Chain подразумевает следующее определение: зная

последовательность действий потенциального нарушителя режима ИБ, обороняющаяся сторона может выработать стратегию защиты и противостоять нападению [6]. Схема Kill Chain представлена на рисунке 1.

Рис. 1. Модель Kill Chain

На этапе разведки потенциальный нарушитель режима ИБ производит сбор информации об организации, которая будет атакована, а также о её информационных активах.

На этапе вооружения потенциальным нарушителем производится оснащение утилитами и системами в целях совершения успешной атаки.

На этапе доставки выполняется перенос вредоносного контента до целевой системы, в роли которой могут выступать информационные системы, информационно–телекоммуникационные сети, а также автоматизированные системы управления.

На этапе заражения выполняется запуск вредоносного кода или эксплуатирует уязвимости системы.

На этапе установки потенциальный нарушитель выполняет открытие удаленного доступа и прочие противоправные действия с зараженной системой.

На этапе получения управления потенциальный нарушитель осуществляет управление зараженной системой;

На последнем этапе выполняется непосредственно сбор, кража, отправка данных, шифрование файлов, подмена и удаление данных.

Важно учитывать, что модель Kill Chain представляет собой цепочку четко заданных последовательных действий**,** поэтому прерывание атаки на любом из ее этапов будет неудачей для злоумышленника. От того, на каком этапе была обнаружена угроза, зависит эффективность результатов управления инцидентом, а также размер материального и репутационного ущерба, нанесенного атакуемой организации.

В целях минимизации серьезного ущерба от возникновения инцидентов ИБ, которые, как было продемонстрировано выше, являются частью модели Kill Chain, необходим грамотно выстроенный процесс реагирования на инциденты ИБ [7]. Приведем графическое отображение процесса реагирования на инциденты ИБ на рисунке 2.

По результатам проведенного анализа схемы можно сделать следующие выводы о результатах выполнения каждого из этапов процесса реагирования на инциденты ИБ:

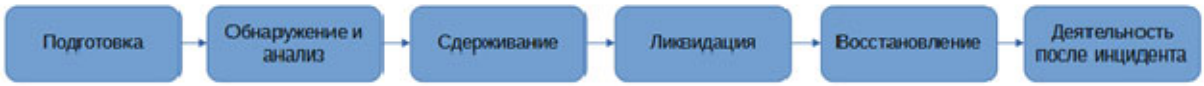

Рис. 2. Процесс реагирования на инциденты ИБ

Этап подготовки к реагированию на инцидент состоит из всех действий, которые могут выполняться до самого инцидента, чтобы лучше справиться с ним. Он включает в себя разработку политики и процедур, регулирующих реагирование и обработку инцидентов, проведение тренингов и обучения как для обработчиков инцидентов, так и для тех, кто должен сообщать об инцидентах, проведение учений по реагированию на инциденты, разработку и ведение документации, и множество других подобных мероприятий. Важность этого этапа реагирования на инциденты не следует недооценивать. Без надлежащей подготовки крайне маловероятно, что реакция на инцидент пройдет хорошо и/или в том направлении, в котором ожидается;

На этапе обнаружения и анализа возможно обнаружить возникновение проблемы и решить, является ли это на самом деле инцидентом, чтобы мы могли отреагировать на него соответствующим образом. Часть обнаружения на этом этапе часто является результатом мониторинга или оповещения на основе выходных данных средства защиты информации или службы безопасности. В качестве вышеуказанных данных могут выступать выходные данные из системы обнаружения вторжений (IDS), антивирусного программного обеспечения, журналов брандмауэра, журналов прокси–сервера, оповещения из средства мониторинга информации и событий безопасности (SIEM);

Этап сдерживания предполагает принятие мер для обеспечения того, чтобы ситуация не причинила большего ущерба, чем она уже причинила, или, по крайней мере, для уменьшения любого продолжающегося ущерба;

Во время этапа ликвидации определяются всех затронутые компьютеры, серверы в организации, чтобы их можно было восстановить;

На этапе восстановления происходит восстановление нормальной работы систем, подтверждение, что системы функционируют нормально, и (если применимо) устраняют уязвимости для предотвращения подобных инцидентов. Восстановление может включать такие действия, как восстановление систем из чистых резервных копий, восстановление систем с нуля, замена скомпрометированных файлов чистыми версиями, установка исправлений, смена паролей и усиление безопасности периметра сети (например, наборы правил брандмауэра, списки контроля доступа пограничных маршрутизаторов);

На этапе деятельности после инцидента пытаются конкретно определить, что произошло, почему это произошло и что можно сделать, чтобы это не повторилось. Цель деятельности после инцидента состоит в

том, чтобы в конечном счете предотвратить или уменьшить последствия будущих подобных инцидентов.

Таким образом, необходимость процесса реагирования на инциденты ИБ связано с тем, что количество инцидентов ИБ растет пропорционально ценности и стоимости информации организации. Для эффективности данного процесса необходимы: анализ предметной области управления инцидентами ИБ, грамотная и оперативная работа сотрудников ИБ на каждом его этапе, проведение тренингов для сотрудников организации, в том числе и сотрудников ИБ, применение актуальной отечественной и мировой нормативно-методической базы, посвященной процессам управления инцидентами ИБ, а также использование современных средств защиты, помогающих в реагирование на инцидент ИБ.

Список литературы

1. ГОСТ Р ИСО/МЭК 27000–2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.

2. What is incident response? | IBM [Электронный ресурс] URL: https://www.ibm.com/topics/incident–response (дата обращения: 14.12.2021).

3. X–Force Threat Intelligence Index 2020 [Электронный ресурс] URL: https://www.ibm.com/security/data–breach/threat–intelligence (дата обращения: 14.12.2021).

4. Аналитика Solar JSOC: как атакуют российские компании / Habr [Электронный ресурс] URL: https://habr.com/en/company/solarsecurity/blog/338330/ (дата обращения: 29.01.2022).

5. Incident Response Process – an overview | ScienceDirect Topics [Электронный ресуср] URL: https://www.sciencedirect.com/topics/computer–science/incident–response–process (дата обращения: 14.12.2021).

6. J. Haseeb, M. Mansoori and I. Welch, "A Measurement Study of IoT-Based Attacks Using IoT Kill Chain", *2020 IEEE 19th International Conference on Trust Security and Privacy in Computing and Communications (TrustCom)*, pp. 557-567, 2020.

7. Отакулов Артур Собирович Способы реагирования на инциденты информационной безопасности // E–Scio. 2020. №1 (40). URL: https://cyberleninka.ru/article/n/sposoby–reagirovaniya–na–intsidenty–informatsionnoy–bezopasnosti (дата обращения: 15.02.2022).

Совгирь Антов Витальевич, студент, sovgir.anton130799@mail.ru, Россия, Тула, Тульский государственный университет,

Чернов Денис Владимирович, кандидат технических наук, доцент, cherncib@gmail.com, Россия, Тула, Тульский государственный университет

ANALYSIS OF INFORMATION SECURITY INCIDENT MANAGEMENT PROCESSES

Sovgir A.V., Chernov D.V.

Abstract: This article examines the most common cyberspace information security incidents in the context of compliance with the model of penetration of a potential violator of the information security regime into an information system. The authors describe the stages of the information security incident response process.

Keywords: information security, incident, Kill Chain, incident management.

Sovir Antov Vitalievich, student, sovgir.anton130799@mail.ru, Russia, Tula, Tula State University,

Chernov Denis Vladimirovich, candidate of technical sciences, associate professor, cherncib@gmail.com, Russia, Tula, Tula State University.

УДК 621.454.3

МЕТОДИЧЕСКИЕ ПОДХОДЫ К ПРОЕКТИРОВАНИЮ ФОРМ НАПОЛНИТЕЛЕЙ В ДВИГАТЕЛЯХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ С МАЛЫМ ОТНОСИТЕЛЬНЫМ УДЛИНЕНИЕМ

Е.С. Германович, С.А. Гусев, В.А. Кулибаба, В.С. Попов, А.И. Шкурин

Работа посвящена исследованию различных форм прочноскрепленных наполнителей, горящих по внутренней поверхности, определению законов изменения их поверхности горения в процессе работы.

Ключевые слова: двигатели летательных аппаратов, поверхность горения.

Многие современные двигатели летательных аппаратов (ДЛА) снаряжаются наполнителями, скреплёнными по наружной поверхности с корпусом камеры сгорания и горящими только по внутреннему каналу, что позволяет исключить длительный контакт высокотемпературных газов с камерой. Форма наполнителя – один из важнейших составляющих ДЛА, оказывающих влияние на габаритно – массовые характеристики, внутрибаллистические и энергетические характеристики, прочность наполнителя и корпуса.

К форме наполнителя предъявляется ряд требований, связанных с обеспечением: максимального заполнения внутреннего объема корпуса, изменения поверхности горения по заданному закону, минимизация остатков массы и др.