УДК 004.056

ИНФОРМАЦИОННАЯ СИСТЕМА АНАЛИЗА СТАТИСТИКИ УГРОЗ, ПОСТУПАЮЩИХ ЧЕРЕЗ USB-УСТРОЙСТВА

Герасев С.В., Елизарова Н.Н.

ФГБОУ ВО «Ивановский государственный энергетический университет имени В.И. Ленина», Иваново, e-mail: gerasev.s@mail.ru, madam.n.elizarova2014@yandex.ru

Информационная система анализа статистики угроз, поступающих через USB-устройства, является программным инструментом, целью данной системы является мониторинг и анализ угроз, поступающих через USB-устройства, с целью обеспечения безопасности систем. Система собирает и отправляет статистические данные о подключенных устройствах и сведения об их изменениях на сервер. Статистические данные включают информацию об изменении состояния файлов, количества угроз и другую информацию на рабочих станциях в компьютерной сети. Используются различные методы статистического анализа, расчета рисков информационной безопасности. Система предоставляет администраторам сети возможность детального изучения угроз за счет гибкой настройки фильтров сортировки и группировки, что позволяет повысить контроль действий каждого конечного пользователя, работающего с USB-устройством, подключенного к сети. Это предоставляет возможность оперативно реагировать на потенциальные угрозы, блокировать доступ к определенным устройствам или принимать другие меры безопасности. Информационная система анализа статистики угроз через USB-устройства имеет большую значимость для защиты компьютерных сетей от вредоносного программного обеспечения и несанкционированного доступа. Использование системы помогает предотвратить утечку конфиденциальной информации и минимизировать риски для безопасности сети и данных.

Ключевые слова: информационная система, USB-устройства, риски информационной безопасности, статистика угроз, статистический анализ

INFORMATION SYSTEM FOR ANALYZING STATISTICS OF DANGERS RECEIVING VIA USB DEVICES

Gerasev S.V., Elizarova N.N.

Ivanovo State Power Engineering University named after V.I. Lenin, Ivanovo, e-mail: gerasev.s@mail.ru, madam.n.elizarova2014@yandex.ru

The information system for analyzing statistics of cybersecurity dangers receiving via USB devices is a software tool, the purpose of this system is to monitor and analyze cybersecurity dangers receiving via USB devices in order to ensure system security. The system collects and sends statistical data about connected devices and information about their changes to the server. Statistical data includes information about changes in the status of files, the number of dangers, etc. on workstations, on a computer network. Various methods of statistical analysis and calculation of information security risks are used. The system provides network administrators with the opportunity to study threats in detail by flexibly configuring sorting and grouping filters, which allows for increased control over the actions of each end user working with a USB device connected to the network. This provides an opportunity to quickly respond to potential threats, block access to certain devices, or take other security measures. An information system for analyzing cybersecurity dangers statistics via USB devices is of great importance for protecting computer networks from malicious software and unauthorized access. Using the system helps to prevent leakage of confidential information and minimize risks to network and data security.

Keywords: information system, USB device, cybersecurity dangers statistics, cybersecurity risks, statistical analysis

Современный период развития общества характеризуется большим объемом информации, поступающей через различные каналы обмена данными. Кроме того, информация, характеризующая информационный или иной продукт или услугу, выступает как форма собственности и, таким образом, имеет определенную ценность. Поэтому вопросы защиты информации становятся особенно актуальными. Данная статья посвящена анализу угроз, поступающих через USB-устройства.

В современном информационном мире USB-устройства продолжают оставаться актуальным способом передачи информации между пользователями в организации с одного компьютера на другой, если иное не предусмотрено в регулирующих документах организации. При передаче данных посредством последовательного интерфейса для подключения периферийных устройств к рабочим станциям существует ряд угроз, среди которых вирусы, троянские программы, нарушения конфиденциальности, целостности, доступности информации, атаки на систему и многое другое. Важно понимать, что использование USB-устройств несет определенные риски, и без должной защиты данные могут быть скомпрометированы [1, с. 31; 2, с. 4]. Одним

из важных инструментов в обеспечении безопасности информации является сбор статистики и дальнейший ее анализ, собираемой с рабочих станций конечных пользователей для обеспечения безопасности информационных систем.

Существует несколько основных методов анализа статистики, с помощью которых можно выявлять закономерности в появлении угроз, анализировать данные об инцидентах безопасности и строить модели для прогнозирования возможных рисков. Это позволяет специалистам по информационной безопасности организации быстро реагировать на новые угрозы и разрабатывать эффективные меры защиты.

1. Статистический анализ

Статистический анализ позволяет выявить закономерности и тенденции в угрозах и инцидентах информационной безопасности. Анализируя данные о типах атак, их распространенности в корпоративном сегменте, специалисты могут выявить наиболее вероятные угрозы и подготовить соответствующие контрмеры.

2. Анализ причинно-следственных связей

Этот метод направлен на выявление причин возникновения инцидентов информационной безопасности. Анализируя цепочку событий, специалисты могут определить источники угроз и уязвимости в системе, что позволяет разрабатывать более эффективные стратегии защиты.

3. SWOT-анализ

SWOT-анализ помогает выявить сильные и слабые стороны системы информационной безопасности, а также возможности для улучшения и угрозы, с которыми следует бороться. Этот метод позволяет специалистам разрабатывать стратегии на основе анализа сильных и слабых сторон компании, внутренних и внешних факторов, оказывающих влияние на деятельность организации.

4. Анализ трендов

Изучение трендов в области информационной безопасности позволяет оперативно реагировать на новые угрозы и уязвимости. Специалисты могут анализировать изменения в методах атак, используемых хакерами, и принимать меры по защите от них [3, с. 19].

Цель исследования – разработка информационной системы мониторинга и сбора статистики угроз, поступающих через USB-устройства, анализ инцидентов, определения рисков угроз, формирование информации для дальнейшего обеспечения безопасности функционирующих систем предприятия.

Материалы и методы исследования

Исследование основано на теоретико-экспериментальном мониторинге угроз и анализе информации об угрозах, инцидентах и попытках несанкционированного доступа к информации через USB-порты. Для обработки информации используются методы статистического анализа, вероятностные методы расчета рисков угроз.

Результаты исследования и их обсуждение

Результаты исследований позволяют выявить элементы, имеющие наибольшее количество инцидентов, оценить риски угроз, что позволяет спланировать мероприятия по информационной безопасности и повысить эффективность функционирования информационных систем организации.

Разработанная информационная система включает задачи мониторинга угроз и инцидентов и их анализа [4]. Основные этапы обработки представлены на рисунке.

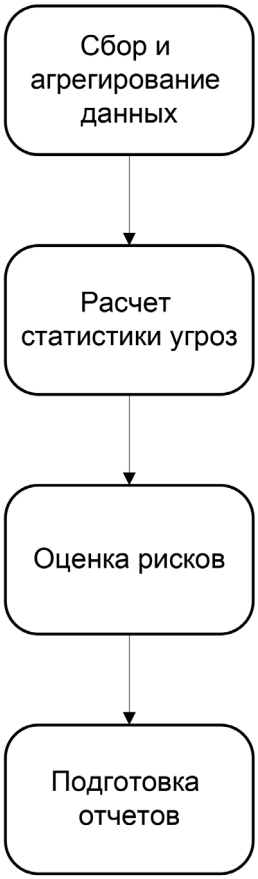
Первым этапом в проведении мониторинга является сбор и агрегация данных о событиях, связанных с использованием USB-устройств. Это включает в себя информацию об обнаруженных угрозах, инцидентах и попытках несанкционированного доступа к информации через USB-порты. Эти данные можно получить с помощью специализированного программного обеспечения (агентов) или систем мониторинга безопасности.

Вторым этапом является анализ полученных данных [5, с. 27]. Статистика угроз позволяет выявить основные тренды и образцы, характерные для организации. Например, это может быть увеличение числа инцидентов за определенный период времени (N_t) или особо активные сотрудники (D_m), которые часто используют USB-устройства для передачи данных. Анализ таких трендов помогает определить факторы, влияющие на безопасность информационной системы.

Третий этап включает в себя оценку рисков и разработку мер по обеспечению безопасности. На основе собранных и проанализированных данных можно выявить уязвимости и определить наиболее подверженные риску области. Это может быть необходимость усилить физическую безопасность, реорганизация процессов обработки данных или внедрение дополнительных систем защиты.

Четвертый этап – подготовка отчетности и мониторинг эффективности мер. Подготовка отчетов для руководства организации с описанием текущего состояния информа-

ционной безопасности и предложениями по улучшению. После внедрения рекомендованных мер следует отслеживать изменения в статистике угроз и инцидентов, чтобы оценить эффективность данных мероприятий.



Этапы мониторинга и анализа угроз

На первом этапе сбора данных о событиях получаем статистики, которые позволяют отслеживать изменения, производимые пользователем на USB-устройстве, подключенном к рабочей станции, собирать информацию о состоянии изменения файлов на устройстве:

$$\text{Status} = \{S_1, S_2, S_3\},$$

где S_1 – перемещение файлов;
S_2 – удаление файлов;
S_3 – изменение файлов.

Данная статистическая функция позволяет собрать общие сведения:

$$\text{OS} = \{\text{Name, Tip, Data, } T_1, T_2\},$$

где OS – общие сведения;
Name – имя пользователя;
Tip – тип файлов;
Data – дата подключения устройства;
T_1 – время подключения устройства;
T_2 – время отключения устройства.

Для выполнения агрегирования к полученным данным можно применять различные фильтры отбора.

Сортировка может проводиться по следующим критериям:

– по конечному пользователю (K_1);
– по группе пользователей (K_2);
– по диапазону времени (как диапазону общего времени, так и времени работы пользователя) (K_3);
– по измененным перемещенным удаленным файлам (K_4);
– по типу расширения файла (K_5);
– по названию файла (K_6);
– по размеру файла (K_7);
– по статусу пользователя (K_8);
– по длительности последнего сеанса (K_9).

Сортировка позволяет ускорить процесс обнаружения и детектирования конечных рабочих станций, на которых были выявлены несанкционированные действия со стороны пользователя, данный блок статистики позволяет в короткое время идентифицировать конечного пользователя, подключающего внешнее устройство посредством USB-портов, тем самым сократить время реагирования на инцидент(противоправную информацию на другие рабочие узлы).

На втором этапе можно подсчитать:

1) статистику работы за определенный период одним пользователем:

$$v_{ij} = \frac{k_{ij}}{\sum_i k_{ij}}, \quad (1)$$

где v_{ij} – доля операций i-го вида (статуса) j-м пользователем;
k_{ij} – количество операций i-го вида;

2) максимальное число инцидентов за определенный период времени:

$$N_t = \max_{t \in [t_{j-1}, t_j]} N_{ij}, \quad (2)$$

где N_{ij} – число инцидентов на j-м интервале;

3) сотрудники, наиболее часто использующие USB-устройства:

$$D_m = \max_j m_{j,} \quad (3)$$

где m_j – количество операций любого вида, выполняемых j-м сотрудником.

Запись об обнаружении вирусов на определенных носителях располагается в следующем статистическом блоке;

4) наиболее зараженные устройства:

$$V_{угр} = \max_j q_{j,} \quad (4)$$

где q_j – количество угроз любого вида, обнаруженных на j-м устройстве.

Данный блок статистики позволяет провести более глубокий анализ использования USB конечным пользователем,

что в свою очередь ускоряет процесс принятия мер в отношении конкретного пользователя не только на уровне блокировки его профиля в системе, но и на организационном уровне учреждения, в случаях, приведших к нарушению работы системы (простой, сбой, зависание и т.п.), а также нарушению конфиденциальности, целостности, доступности информации в системе. Данная статистическая функция в связке с первой позволяет рассчитать ущерб организации за период простоя системы и возложить ответственность на лиц, ответственных за информационную безопасность предприятия.

В результате статистического анализа все компоненты можно группировать по следующим основаниям:

− наиболее зараженные устройства (показывает устройство, пользователя и количество обнаруженных вирусов на этом устройстве);

− группа риска (показывает пользователей, на устройствах которых было обнаружено наибольшее количество угроз);

− активные пользователи (показывает данные по пользователям, общее время их работы с подключенным устройством через последовательный интерфейс для подключения периферийных устройств, общее количество измененных, удаленных, перемещенных файлов, наиболее часто изменяемый формат файлов);

5) наиболее заражающие пользователи:

$$D_m = \max_j q_{j,} \qquad (5)$$

где q_j – количество угроз любого вида, обнаруженных на устройствах j-го сотрудника.

Данный блок статистики показывает пользователей, на устройствах которых было обнаружено наибольшее количество угроз, что позволяет администратору информационной безопасности сформировать группы, с которыми необходимо проводить дополнительные мероприятия, касающиеся вопросов информационной безопасности предприятия. Важно отметить, что обучение и информирование пользователей являются ключевыми моментами в обеспечении безопасности информации в организации. Предоставление сотрудникам необходимых знаний и навыков в области информационной безопасности поможет снизить риск заражения и повысить уровень защиты системы от киберугроз. Таким образом, данный блок статистики дополняет предыдущие блоки непосредственной идентификацией конечного пользователя, что позволяет сделать более качественный анализ угроз информационной безопасности предприятия [6, с. 45; 7].

На третьем этапе определяем перечень информационных угроз, которые могут сформироваться и негативно воздействовать на объекты информационной системы:

- Y_1 – утечка информации;
- Y_2 – нежелательный контент;
- Y_3 – потеря данных.

Риски R_i угроз Y_i нанесения ущерба информационным объектам O_i можно определить по формуле

$$R_i = P_i \times \sum_j P_{ij} \times S_j , \qquad (6)$$

где P_i – вероятность реализации угрозы Y_i информационной безопасности;

P_{ij} – вероятность уязвимости объекта O_j угрозой Y_i;

S_j – ущерб объекта O_j от реализации угроз информационной безопасности.

Сбор и анализ данных статистики событий при использовании устройств, подключаемых к USB-портам, позволяет осуществить поиск уязвимых зон для оценки степени влияния угроз на функционирования компании, своевременно выявлять нарушения, связанные с информационной безопасностью организации, и уменьшить вероятности уязвимости P_{ij} и вероятности реализации угроз P_i, что приводит к снижению рисков R_i [8, с. 36; 9]. На основе этой информации может быть построена матрица угроз $||P||$ как сводная таблица, отражающая вероятности возникновения угроз и степени их влияния.

Заключение

Статистический анализ угроз нарушений является важным инструментом в обеспечении информационной безопасности любой организации. Правильное применение статистических методов позволяет оценить вероятность наступления определенных событий и принимать обоснованные решения по обеспечению безопасности данных. Понимание и правильная настройка статистических выборок помогают специалистам по информационной безопасности эффективно защищать ценные информационные ресурсы компании.

Важно отметить, что после внедрения мер по обеспечению безопасности необходимо провести повторный анализ, чтобы оценить их эффективность и внести необходимые корректировки. USB-устройства постоянно совершенствуются, и угрозы, связанные с их использованием, могут изменяться. Анализ статистики угроз, передающихся посредством подключения устройств к последовательному интерфейсу в организации, является неотъемлемой частью обеспечения безопасности инфор-

мационных систем. Он позволяет выявить основные тренды и риски, а также разработать эффективные меры по их предотвращению и устранению. Систематический подход к анализу статистики гарантирует безопасность и сохранность данных. На основе анализа всех статистических блоков можно сформировать подробное представление и разработать комплексный подход по обеспечению информационной безопасности связанных с защитой каналов передачи данных посредством USB-подключений, целесообразности ужесточения или смягчения мер.

Список литературы

1. Краковский Ю.М. Методы и средства защиты информации: учебное пособие для вузов. СПб.: Лань, 2024. 272 с.

2. Киренберг А.Г., Коротин В.О. Защита информации от утечки по техническим каналам: учебное пособие. Кемерово: КузГТУ имени Т.Ф. Горбачева, 2023. 222 с.

3. Абденов А.Ж., Белкин С.А., Заркумова-Райхель Р.Н. Методика оценки риска для информационных систем на основе экспертных оценок: учебное пособие. Новосибирск: НГТУ, 2014. 71 с.

4. Рудаков Н.В., Герасев С.В. Разработка программного комплекса регистрации неправомерного доступа к рабочим станциям посредством USB-устройств // Молодой исследователь 2024: сборник статей IV Международной научно-практической конференции. Пенза: МЦНС «Наука и Просвещение», 2024. С. 41–45.

5. Белов А.А., Баллод Б.А., Елизарова Н.Н. Прикладные теории вероятностей и математическая статистика: учебное пособие. Иваново: ФГБОУ ВО «Ивановский государственный энергетический университет имени В.И. Ленина», 2019. 184 с.

6. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление инцидентами информационной безопасности и непрерывностью бизнеса: учебное пособие для вузов. 2-е изд. М.: Гор. линия – Телеком, 2016. 170 с.

7. Крутова Н.А., Крутов А.Н., Иванчина О.В. Проблема анализа рисков в управлении информационной безопасностью предприятия // Вестник СамГУПС. 2019. № 1 (43). С. 96–103.

8. Царегородцев А.В., Романовский С.В., Волков С.Д. Анализ рисков в процессах обеспечения информационной безопасности жизненного цикла финансовых автоматизированных информационных систем: монография. М.: ИНФРА-М, 2024. 198 с.

9. Бакин И.Б., Ниязова К.Ш., Шведова С.М. Проблемы управления рисками в сфере информационной безопасности // Вестник РГГУ. Серия: Информатика. Информационная безопасность. Математика. 2023. № 3. С. 49–60.