УДК 004.056.5

Сапронов Андрей Анатольевич - *студент, Высшая инженерная школа Российского университета транспорта (МИИТ),*
e-mail: AndreyCotic@yandex.ru

ПРИМЕНЕНИЕ РЕСУРСА ZEEK ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В статье будет рассмотрено создание системы защиты информации для органов государственной власти. Будет обосновано создание системы управления доступом к классифицированной информации и внедрение криптографии для передачи данных в государственных структурах. Информационная безопасность — это комплекс мер и методов, направленных на защиту информации от несанкционированного доступа, использования, раскрытия, разрушения или модификации. Значение информационной безопасности в современном мире трудно переоценить, и оно включает в себя несколько ключевых аспектов. В условиях быстрого развития технологий и увеличения числа киберугроз информационная безопасность становится неотъемлемой частью стратегии управления рисками любой организации. Результатом статьи является разработка способа внедрения ресурса Zeek для защиты информации с обоснованием эффективности использования данного ресурса.

Abstract. The article will consider the creation of an information security system for public authorities. The creation of an access control system for classified information and the introduction of cryptography for data transmission in government agencies will be justified. Information security is a set of measures and methods aimed at protecting information from unauthorized access, use, disclosure, destruction or modification. The importance of information security in the modern world cannot be overestimated, and it includes several key aspects. With the rapid development of

technology and the increasing number of cyber threats, information security is becoming an integral part of any organization's risk management strategy. The result of the article is the development of a method for implementing the Zeek resource to protect information, justifying the effectiveness of using this resource.

Ключевые слова: информационная безопасность, киберугрозы, криптография, шифрование, государственная власть, средства защиты информации, Zeek.

Keywords: information security, cyber threats, cryptography, encryption, government power, information security tools, Zeek.

Функционирование органов государственной власти — это сложный процесс, который включает в себя организацию работы различных институтов и их взаимодействие в рамках правового и политического поля. Оно требует постоянной адаптации к изменяющимся условиям и вызовам, включая экономические, социальные и политические факторы.

История развития информационных технологий (ИТ) в деятельности органов государственной власти проходит через несколько ключевых этапов.

Первые компьютеры начали использоваться в государственных учреждениях в середине XX века. В этот период ИТ использовались преимущественно для обработки данных и выполнения рутинных операций, таких как бухгалтерский учет или статистическая обработка.

С развитием персональных компьютеров и программного обеспечения, органы государственной власти начали активно автоматизировать свои процессы. Появление специализированных программных решений для управления документами и общественными услугами стало важным шагом к повышению эффективности работы государственных структур.

С распространением интернета началась так называемая эпоха электронного правительства (e-government). Государственные органы начали создавать свои веб-сайты для предоставления информации и услуг гражданам. Это позволило улучшить доступность государственных услуг и повысить уровень информированности населения.

Начиная с XXI века происходит активная цифровая трансформация. Развиваются системы межведомственного электронного взаимодействия, электронные базы данных, а также различные цифровые инструменты для взаимодействия с гражданами. Появляются мобильные приложения для получения государственных услуг, электронные личные кабинеты и системы "умного города".

Современные органы власти активно используют большие данные, искусственный интеллект и блокчейн для повышения прозрачности и эффективности. Важной тенденцией становится создание умных городов, где ИТ активно внедряются в управление городским хозяйством, транспортом и инфраструктурой.

Таким образом, информационные технологии становятся неотъемлемой частью современной государственной деятельности, обеспечивая её эффективность, прозрачность и доступность.

Цифровизация органов государственной власти, несмотря на многие положительные аспекты, также может иметь ряд негативных последствий, примером таких последствий являются: угрозы безопасности данных, цифровое неравенство, зависимость от технологий, отсутствие прозрачности, монополизация технологий, ограничение прав на информацию, и.т.д.

Эти последствия требуют внимательного рассмотрения при реализации программ цифровизации, чтобы минимизировать риски и обеспечить более эффективное взаимодействие органов государственной власти с гражданами.

Особое внимание необходимо уделить угрозам безопасности данных – то есть подробно описать работу органов государственной власти с точки зрения информационной безопасности. Опишем известные на данный момент способы нарушения информационной безопасности, представляющие угрозу для данных:

•Вирусы и Malware: вредоносные программы, которые проникают в систему с целью повреждения данных, отключения оборудования или кражи конфиденциальной информации.

•Фишинг: техника обмана пользователей, при которой злоумышленники пытаются получить личные данные, например, пароли или номер кредитной карты, путем маскировки под legitimate-сервис.

•Атаки с использованием нулевых дней: эксплуатация уязвимостей программного обеспечения, которые еще не были обнаружены разработчиками и, соответственно, не имеют патчей или обновлений для защиты.

•DDoS-атаки (распределенные атаки отказа в обслуживании): атаки с использованием множества источников для перегрузки сервера или сети, что приводит к недоступности услуги для легитимных пользователей.

•Несанкционированный доступ: проникновение в системы или сети без разрешения, что может привести к утечке чувствительной информации или повреждению данных.

•Социальная инженерия: манипуляция людьми с целью получения конфиденциальной информации. Включает в себя обман, подмену реальности и использование доверия.

•Вынос данных: атаки, которые направлены на кражу или утечку конфиденциальной информации из системы, включая финансовые данные и личные данные пользователей.

•Уязвимости программного обеспечения: логические или физические слабости в программных системах, которые могут быть использованы злоумышленниками для получения несанкционированного доступа.

•Кража идентификации: процесс получения и использования личной информации с намерением обмануть, например, для открытия кредитной линии или доступа к банковским счетам.

•Инсайдерские угрозы: угрозы, исходящие от сотрудников или индивидуумов с легитимным доступом к информации, которые могут намеренно или случайно скомпрометировать безопасность данных.

•Инфраструктурные атаки: нападения на критически важную инфраструктуру, такие как системы энергоснабжения, которые могут привести к серьезным последствиям.

•Бэкдоры и эксплойты: скрытые уязвимости в программных системах, которые позволяют злоумышленникам получить доступ без потребности в стандартных аутентификационных данных.

•Потеря данных: неправомерная утечка или потеря данных из-за сбоев оборудования, человеческих ошибок или вредоносных действий.

Нарушение информационной безопасности в государственных структурах может иметь серьезные последствия, включая:

•Утечка конфиденциальной информации: порой это может касаться личных данных граждан, государственной тайны или секретной информации, что может привести к юридическим и моральным последствиям.

•Утрата доверия со стороны граждан: граждане могут потерять доверие к государственным учреждениям, если станет известно о нарушениях безопасности, что может снизить их готовность сотрудничать с государством.

•Финансовые потери: устранение последствий инцидентов информационной безопасности требует значительных финансовых ресурсов, включая расходы на аудит, восстановление данных, улучшение систем безопасности и возможные юридические издержки.

•Политические последствия: в некоторых случаях утечка информации может привести к политическим кризисам выборах и дестабилизации политической системы.

•Угрозы национальной безопасности: в случае несанкционированного доступа к критически важной информации возможны угрозы для национальной безопасности, включая шпионаж и террористические акты.

•Юридические последствия: государственные структуры могут столкнуться с судебными исками как со стороны граждан, так и со стороны других организаций, что может привести к дополнительным штрафам и санкциям.

•Увеличение киберугроз: успешные атаки могут стимулировать других злоумышленников к попыткам нарушить безопасность, создавая порочный круг атак.

Для минимизации рисков нарушения информационной безопасности государственные структуры должны инвестировать в средства защиты информации, обучение сотрудников и разработку стратегий реагирования на инциденты.

Обеспечение информационной безопасности требует комплексного подхода, включающего технологии, политики, обучение сотрудников и постоянный мониторинг угроз.

Принимая во внимание вышеописанные факторы, становится очевидным, что органы государственной власти уделяют внимание обеспечению информационной безопасности своих ресурсов. Представим эти методы на Рисунке 1.

Рисунок 1 – Основные методы обеспечения информационной безопасности, применяемые органами государственной власти

Эти меры комплексно направлены на защиту информационных ресурсов, обеспечение их конфиденциальности, целостности и доступности. Необходимо отметить, что даже совокупность методов не может полностью исключить возможность киберугроз. Так, процедура принятия нормативно-правовых актов

может длиться годами, в то время как технологии развиваются гораздо быстрее, что делает принимаемые законы и стандарты неэффективными. Многие алгоритмы шифрования достаточно быстро устаревают, что влияет на выполнение их функций. Зачастую люди до сих пор не уделяют должного внимания цифровой гигиене, что делает неэффективными методы, связанные с человеческим фактором.

Прежде всего следует отметить, что предложенная система защиты информации не должна противоречить действующему законодательству, а именно: Конституции РФ [3], Федеральному закону № 149-ФЗ "Об информации, информационных технологиях и о защите информации" [4], Федеральному закону № 152-ФЗ "О персональных данных" [5], Федеральному закону № 187-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)"[6], Приказам ФСТЭК (Федеральная служба по техническому и экспортному контролю): Приказ № 21 — Требования к СЗИ (системам защиты информации) в госструктурах [7], Приказ № 31 — Правила противодействия угрозам с использованием VPN и анонимных сетей [8], Приказ № 239 — Методика оценки рисков для КИИ [9], Приказам ФСБ (Федеральная служба безопасности): Приказ № 378 — Требования к криптографической защите информации [10], Приказ № 515 — Правила использования электронных подписей [11].

Для модернизации систем защиты информации в госсекторе предлагается использовать систему обнаружения вторжений (СОВ) Zeek (далее-Zeek).

Zeek — это open-source-решение для анализа сетевого трафика. Одним из главных преимуществ Zeek является предоставление большого набора log-файлов. Каждый log-файл содержит в себе определенную сетевую смысловую нагрузку: HTTP-сессии, DNS-запросы, TLS-соединения, информацию о TLS-сертификатах и многое другое. В дополнение к журналам, Zeek имеет встроенные утилиты для различного рода задач анализа и обнаружения. Zeek может извлекать файлы из HTTP-сессий, обнаруживать вредоносное ПО путем взаимодействия с внешними реестрами, сообщать об уязвимых версиях программного обеспечения, обнаруженных в сети, идентифицировать

популярные веб-сайты, приложения и другие ресурсы. Zeek представляет собой настраиваемую и расширяемую платформу для работы с трафиком. Стоит отметить, что Zeek работает на стандартном оборудовании и, следовательно, представляет собой хорошую альтернативу дорогим решениям. Zeek специально ориентирован на высокоскоростной мониторинг сети в больших объемах. Zeek написан на языке C++ и распространяется под лицензией BSD.

Архитектура Zeek представлена на Рисунке 2.

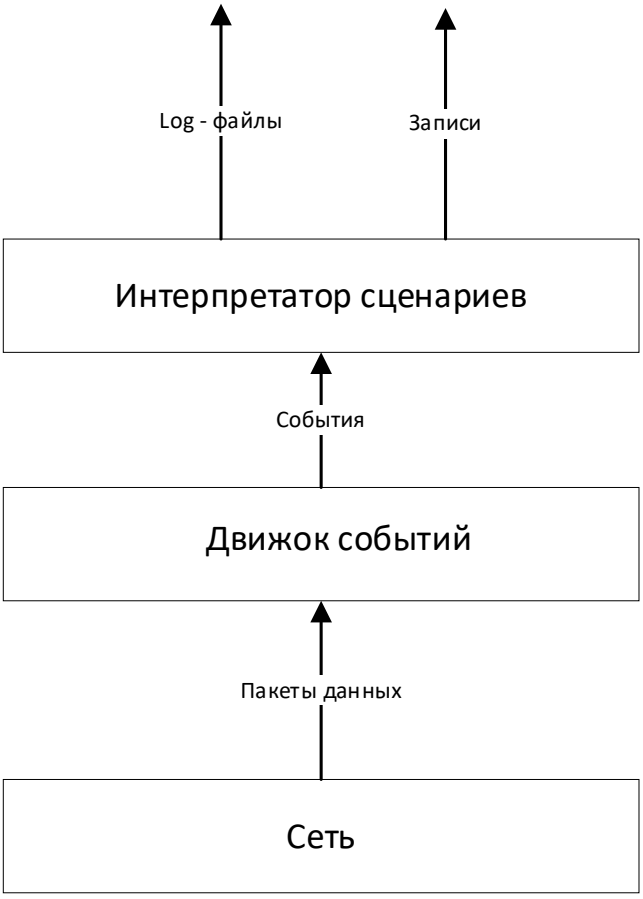

Рисунок 2 – Архитектура Zeek

Архитектура Zeek разделена на два основных компонента. Первый компонент – это Event Engine (движок событий). Он разделяет сетевой пакет на несколько высокоуровневых событий. Эти события отражают сетевую активность, т.е. они описывают то, что было замечено в сетевом пакете. Event Engine включает в себя ряд подкомпонентов: источники ввода, анализ пакетов, анализ сессий и анализ файлов. Анализ пакетов обрабатывает протоколы более низкого уровня, начиная с канального уровня. При анализе сессий проверяются

протоколы прикладного уровня, такие как HTTP, FTP и т.д. При анализе файлов анализируется содержимое файлов, передаваемых во время сессии. Движок событий предоставляет архитектуру плагинов, которые позволяют расширять возможности Zeek по мере необходимости. Вторым основным компонентом Zeek является интерпретатор сценариев Policy Script Interpreter, который выполняет набор обработчиков событий, написанных на скриптовом языке-ассемблере Zeek. Данные скрипты могут мониторить различную активность в сети и в процессе, например, выполнить внешнюю программу.

Для запуска в командной строке Zeek можно выполнить команду, которая отслеживает трафик на интерфейсе*: zeek –i eth0*.

Рассмотрим записи трафика в формате JSON. Пример log-файлов в таком формате представлен на Рисунке 3.

```
vas@debian:~$ cat conn.log | jq | head -n 50
{
  "ts": 1737910148.370016,
  "uid": "CNkeFB44VDdbBeD929",
  "id.orig_h": "192.168.1.101",
  "id.orig_p": 41628,
  "id.resp_h": "104.26.4.62",
  "id.resp_p": 443,
  "proto": "tcp",
  "conn_state": "OTH",
  "local_orig": true,
  "local_resp": false,
  "missed_bytes": 0,
  "history": "C",
  "orig_pkts": 0,
  "orig_ip_bytes": 0,
  "resp_pkts": 0,
  "resp_ip_bytes": 0
}
```

Рисунок 3 – Пример представления log-файлов в формате JSON

ts – это время получения первого пакета, proto – протокол транспортного уровня, conn_state – состояние соединения, local_orig – логическое значение (true или

false), которое показывает локальное (t) ли соединение или удаленное (f), local_resp - логическое значение (t или f), которое показывает ответ из локальной сети (t) или из удаленной (f).

Скрипты можно запускать из командной строки. После выполнения создается папка со скриптом, тестами и другой служебной информацией.

Покажем работу Zeek на примере небольшой сети. Топология сети, в которой была протестирована работа Zeek, представлена на Рисунке 4.

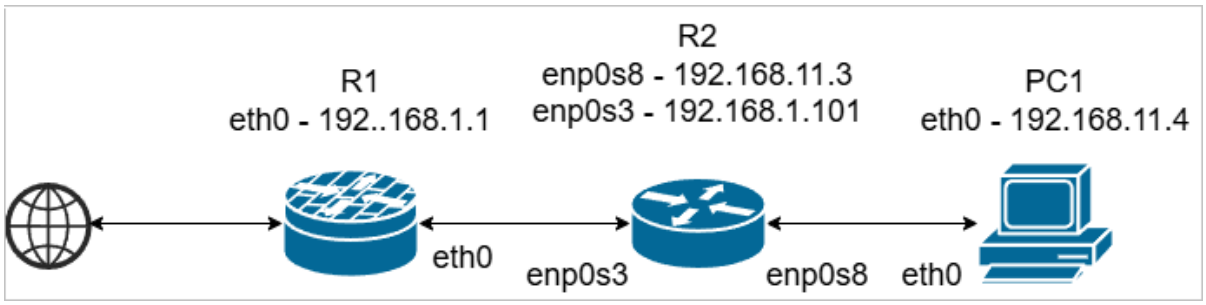

Рисунок 4 – Топология тестируемой сети

На маршрутизаторе R2 стоял Zeek – сенсор. Он прослушивает интерфейс enp0s8. На маршрутизаторе R1 прописан маршрут до сети 192.168.11.0/24 через 192.168.1.101. В качестве R2 была взята обычная машина с операционной системой Debian, на которой была настроена маршрутизация сетевых пакетов.

Результатом выполнения команд, ответственных за анализ сетевого трафика, являются записи в файле app.log, отображающие сетевую активность на рабочей станции PC1. Эти записи представлены на Рисунке 5.

```
#unset_field    -
#path   app
#open   2025-02-01-10-49-11
#fields time_hum        id.orig_h       id.orig_p       id.resp_h  id.resp_p       ser
ver_name
#types  string  addr    port    addr    port    string
2025-02-01, 10:49:11    192.168.11.4    39082   77.88.55.242       443     ya.ru
2025-02-01, 10:49:18    192.168.11.4    46124   108.177.14.113     443     google.com
2025-02-01, 10:49:29    192.168.11.4    39730   62.217.160.2       443     dzen.ru
2025-02-01, 10:49:36    192.168.11.4    40668   140.82.121.3       443     github.com
2025-02-01, 10:49:56    192.168.11.4    53046   77.88.55.88443     yandex.ru
2025-02-01, 10:50:05    192.168.11.4    34080   94.100.180.200     443     mail.ru
2025-02-01, 10:50:22    192.168.11.4    48030   209.85.233.190     443     youtube.com
2025-02-01, 10:51:01    192.168.11.4    33494   93.186.225.194     443     vk.ru
```

Рисунок 5 – сетевая активность на рабочей станции PC1

Как видно из log-файла, Zeek успешно анализирует TLS трафик. Также Zeek пишет свой log-файл, в котором пишется информация о добавленных и удалённых правилах, а также о инициализации плагина.

Предложенное решение обладает рядом преимуществ над используемыми на сегодняшний день способами защиты информации в органах государственной власти РФ. Так, благодаря open-source, можно кастомизировать и адаптировать систему под нужды государственной власти и действующее Российское законодательство, что не является характерной чертой многих действующих средств защиты информации (СЗИ). Большое количество предоставляемых log-файлов даёт возможность охватить широкий спектр киберугроз, а, соответственно, и предотвратить их. Существует возможность извлечения файлов из HTTP-сессий, обнаружения вредоносного ПО, сообщения об уязвимых версиях программного обеспечения, идентификации популярных сайтов и приложений. Предложенная система предоставляет пользователям объектно-ориентированный язык сценариев для решения множества аналитических задач. Zeek поддерживает задачи, выходящие за рамки кибербезопасности, включая измерение производительности и устранение неполадок, к тому же система способна достичь необходимой производительности на любом компьютере, поэтому является достаточно доступным средством по цене.

Значение человеческого фактора в данной СЗИ уменьшается благодаря широкому функционалу Zeek и возможности прописывать правила и создавать иерархический порядок доступа к информации.

Криптографическая защита передачи данных может осуществляться на основе квантовых технологий, в частности – при помощи технологи квантового распределения ключей (КРК), подробно о возможности применения КРК рассказано в работе [2]. Принцип действия такой технологии можно перенести с отрасли железнодорожного транспорта на компьютерное оборудование госслужащих. Функционал Zeek позволяет применять шифрование, что

значительно упростит задачу внедрения криптографической защиты информации.

Таким образом, можно сделать вывод, что предложенное решение обладает рядом функциональных, инструментальных и экономических преимуществ. Однако стоит отметить, что использование open-source ресурсов в госсекторе на текущий момент ограничено из-за необходимости использования лицензионного ПО согласно действующему законодательству. Поэтому, наряду с разработкой такой системы законодательной ветви власти рекомендуется подготовить правовую базу, позволяющую свободно использовать такие ресурсы как Zeek, поскольку большинство СЗИ разработаны и лицензированы государствами, входящими в перечень иностранных государств и территорий, совершающих недружественные действия в отношении Российской Федерации, Российских юридических и физических лиц. Внедрение предложенной системы поможет в реализации стратегии цифрового суверенитета РФ в столь важном направлении как обеспечение информационной безопасности органов государственной власти.

Литература

1) Гайд по использованию Zeek: https://docs.zeek.org/projects/package-manager/en/stable/index.html
2) Сапронов А.А. Тарадин Н.А. Повышение безопасности функционирования систем диспетчерского управления при передаче информации на основе квантовых технологий // Современные информационные технологии Сборник научных статей 11-й Международной научно-технической конференции. - Бургас, Болгария: Славянский Мир, 2024. - С. 414-419.
3) Конституция Российской Федерации
4) Федеральный закон № 149-ФЗ "Об информации, информационных технологиях и о защите информации"
5) Федеральный закон № 152-ФЗ "О персональных данных"

6) Федеральный закон № 187-ФЗ "О безопасности критической информационной инфраструктуры (КИИ)"
7) Приказы ФСТЭК (Федеральная служба по техническому и экспортному контролю): Приказ № 21 — Требования к СЗИ (системам защиты информации) в госструктурах.
8) Приказ № 31 — Правила противодействия угрозам с использованием VPN и анонимных сетей.
9) Приказ № 239 — Методика оценки рисков для КИИ.
10) Приказы ФСБ (Федеральная служба безопасности):
Приказ № 378 —Требования к криптографической защите информации.
11) Приказ № 515 — Правила использования электронных подписей
12) Росс Андерсон: "Безопасность информационных систем"
13) Перечень недружественных РФ государств

Literature

1) Guide to using Zeek: https://docs.zeek.org/projects/package-manager/en/stable/index.html
2) Sapronov A.A. Taradin N.A. Improving the safety of dispatching control systems for information transmission based on quantum technologies // Modern information technologies Collection of scientific articles of the 11th International Scientific and Technical Conference. - Burgas, Bulgaria: Slavyansky Mir, 2024. - pp. 414-419.
3) Constitution of the Russian Federation
4) Federal Law No. 149-FZ "On Information, Information Technologies and Information Protection"
5) Federal Law No. 152-FZ "On Personal Data"
6) Federal Law No. 187-FZ "On the Security of Critical Information Infrastructure (CII)"
7) Orders of the FSTEC (Federal Service for Technical and Export Control): Order No. 21 — Requirements for Information Security Systems in government agencies.

8) Order No. 31 — Rules for Countering Threats using VPNs and Anonymous Networks.
9) Order No. 239 — Risk assessment methodology for CII.
10) Orders of the FSB (Federal Security Service): Order No. 378 — Requirements for cryptographic protection of information.
11) Order No. 515 — Rules for the use of electronic signatures
12) Ross Anderson: "Information system security"
13) List of states unfriendly to the Russian Federation