АНАЛИЗ ПОТЕНЦИАЛЬНЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ В РЕЗУЛЬТАТЕ ОСУЩЕСТВЛЕНИЯ СТЕГАНОГРАФИЧЕСКИХ АТАК

М.Ю. Федосенко, *Национальный исследовательский университет ИТМО, аспирант, fedosenkomaksim98@gmail.com.*

УДК 004.056

Аннотация. Данная работа представляет собой обзор и анализ угроз информационной безопасности, осуществление которых прямо или косвенно возможно в результате применения злоумышленниками методов стеганографии в корыстных целях. Данные угрозы были взяты из Банка данных угроз информационной безопасности ФСТЭК России. В работе представлено их описание, выделен потенциальный злоумышленник и объект его воздействия. В результате получены основные вектора атак злоумышленников, а также наиболее уязвимые компоненты информационной инфраструктуры предприятия для данного вида атак.

Ключевые слова: информационная безопасность; угрозы; стеганография; БДУ ИБ ФСТЭК; нарушение целостности информации; нарушение доступности информации; нарушение конфиденциальности информации.

ANALYSIS OF POTENTIAL THREATS TO INFORMATION SECURITY OF ENTERPRISE COMPUTER INFRASTRUCTURE AS A RESULT OF STEGANOGRAPHIC ATTACKS

M. Fedosenko, *National Research University.*

Annotation. This work is a review and analysis of information security threats, the implementation of which is directly or indirectly possible as a result of the use of steganography methods by attackers for personal gain. These threats were taken from the Data Bank of Information Security Threats of the FSTEC of Russia. The work presents their description, identifying a potential attacker and the object of his influence. As a result, the main attack vectors for attackers were obtained, as well as the most vulnerable components of an enterprise's information infrastructure to this type of attack.

Keywords: information security; threats; steganography; BDU IS FSTEC; information integrity; information availability; information confidentiality.

Введение

В настоящее время практически каждое предприятие имеет компьютерную инфраструктуру. Она же, в свою очередь, является одной из главных целей нарушителей при осуществлении атак, направленных на предприятие. Это обусловлено тем, что компьютерные инфраструктуры предприятий содержат большое количество цифровых данных и обеспечивают стабильность работы многих компонентов. Нарушение данной стабильности, а именно нарушение целостности, доступности и конфиденциальности процесса работы систем и хранящейся на них информации, способна привести к финансовым и репутационным потерям [1]. Поэтому немаловажной задачей достижения качества и стабильности бизнес – процессов предприятия является задача обеспечения качественного уровня информационной и компьютерной безопасности.

Задача защиты информации известна с давних времен. В разные эпохи развития общества ее решали разными способами. Одним из самых важных подходов является шифрование, в последствии чего появилась наука криптография [2]. Однако с процессом перехода общества от индустриального в постиндустриальное, который выражается в его цифровизации, объемы информации и способов ее обмена значительно увеличились, что привело к увеличению способов атак злоумышленников. В своих атаках хакеры применяют все более новые и изощренные способы, одним из которых является использование стеганографии – метода сокрытия злонамеренной информации внутри легитимной. В среде специалистов в области информационной безопасности уже известны случаи применения стеганографии при реализации компьютерных атак, а также для обмена преступными данными [3]. Одним из самых громких примеров является сокрытие информации в фотографиях, размещенных на сайте *Ebay* террористической группировкой «Аль-Каида» [4].

Целью данной работы является анализ угроз информационной безопасности, реализация которых возможна при применении злоумышленником методов стеганографии в процессе осуществления компьютерных атак. Для достижения поставленной цели необходимо решить следующие задачи:

1. Рассмотреть имеющиеся данные об угрозах информационной безопасности согласно открытому банку данных ФСТЭК,
2. Установить нарушителя и объект его атаки в рамках атакуемой информационной системы,
3. Определить потенциал злоумышленника и вектор атаки на основе объекта атаки и деструктурирующего воздействия,
4. Проанализировать действия злоумышленника и возможные деструктурирующие воздействия на информационную систему,
5. Сравнить полученные результаты, оценить перспективы реализации представленных угроз.

Угрозы информационной безопасности

Для сравнения потенциальных угроз информационной безопасности, возможных в результате стеганографических атак, обратимся к Банку данных угроз от ФСТЭК России [5]. Он представляет собой сборник сведений об основных угрозах и уязвимостях, которые характерны для автоматизированных систем управления, государственных информационных систем. Банк угроз ФСТЭК, помимо названия и кода угрозы, содержит ее краткое описание, вероятные источники, объекты воздействия и, конечно, последствия, которые повлечет за собой реализация угрозы. Первоначальной целью создания банка угроз ФСТЭК являлось повышение информированности специалистов ИБ о существующих угрозах безопасности информации в автоматизированных системах. В основном он использовался заказчиками, операторами, разработчиками информационных систем и систем защиты, применялся лабораториями и органами сертификации средств защиты информации [6].

Что касается проблемы скрытого обмена данных, то ФСТЭК России выделяет под нее конкретную угрозу – УБИ.111 «Угроза передачи данных по скрытым каналам» [7]. Суть ее заключается в возможности осуществления нарушителем неправомерного вывода защищаемой информации из системы, а также передачи управляющих команд путем ее нестандартного (незаметного, скрытого) размещения в легитимно передаваемых по сети (или сохраняемых на отчуждаемые носители) открытых данных путем ее маскирования под служебные протоколы, сокрытия в потоке других данных

(стеганография), использования скрытых пикселей («пикселей отслеживания»). Данная угроза обусловлена недостаточностью мер защиты информации от утечки, а также контроля потоков данных. Реализация возможна при:

1. Наличии у нарушителя прав в дискредитируемой системе на установку специализированного программного обеспечения, реализующего функции внедрения в пакеты данных, формируемых для передачи в системе, собственной информации;
2. Доступа к каналам передачи данных;
3. Посещении пользователем сайтов в сети интернет и открытия электронных писем, содержащих скрытые пиксели.

Однако, помимо явно выделенной в базе данных от ФСТЭК угрозы, связанной непосредственно с скрытым обменом данных, существуют также угрозы, имеющие к ней косвенное отношение. Это обусловлено тем, что наличие данных угроз может являться следствием осуществления атак с использованием скрытых каналов связи. Среди таких угроз можно выделить следующие:

- Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением (УБИ.068) [8]: Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на *API* в целях реализации функций, изначально не предусмотренных дискредитируемым приложением (например, использование функций отладки из состава *API*). Данная угроза обусловлена наличием слабостей в механизме проверки входных данных и команд *API*, используемого программным обеспечением.

  Реализация данной угрозы возможна в условиях:

  – Наличия у нарушителя доступа к *API.*

  – Отсутствия у дискредитируемого приложения механизма проверки вводимых данных и команд.
- Угроза неправомерных действий в каналах связи (УБИ.069) [9]: Угроза заключается в возможности внесения нарушителем изменений в работу сетевых протоколов путем добавления или удаления данных из информационного потока с целью оказания влияния на работу дискредитируемой системы или получения доступа к конфиденциальной информации, передаваемой по каналу связи. Данная угроза обусловлена слабостями сетевых протоколов, заключающимися в отсутствии проверки целостности и подлинности получаемых данных.

  Реализация данной угрозы возможна:

  − При условии осуществления нарушителем несанкционированного доступа к сетевому трафику.
- Угроза несанкционированного копирования защищаемой информации (УБИ.088) [10]: Угроза заключается в возможности неправомерного получения нарушителем копии защищаемой информации путем проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съемный носитель (или в другое место, доступное нарушителю вне системы). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации и контроля доступа лиц в контролируемой зоне.

  Реализация данной угрозы возможна в случае:

– Отсутствия криптографических мер защиты или снятия копии в момент обработки защищаемой информации в нешифрованном виде.

- Угроза подмены содержимого сетевых ресурсов (УБИ.130) [11]: Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемым данным пользователей сети или проведения различных мошеннических действий путем скрытной подмены содержимого хранящихся (сайты, веб-страницы) или передаваемых (электронные письма, сетевые пакеты) по сети данных. Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности содержимого электронного сообщения.

  Реализация данной угрозы возможна при условии:

  – Наличия у нарушителя прав на доступ к сетевым ресурсам.

  – Отсутствии у пользователя сети мер по обеспечению их целостности.

- Угроза пропуска проверки целостности программного обеспечения (УБИ.145) [12]: Угроза заключается в возможности внедрения нарушителем в дискредитируемую систему вредоносного программного обеспечения путем обманного перенаправления запросов пользователя или его программ на собственный сетевой ресурс, содержащий вредоносное программное обеспечение, для его «ручной» или «автоматической» загрузки с последующей установкой в дискредитируемую систему от имени пользователя или его программ. Данная угроза обусловлена слабостями механизмов проверки целостности файлов программного обеспечения и/или проверки подлинности источника их получения.

  Реализация данной угрозы возможна при условии успешного использования обманных техник одного из следующих методов:

  – «Ручного метода» – нарушитель, используя обманные механизмы, убеждает пользователя перейти по ссылке на сетевой ресурс нарушителя, что приводит к запуску вредоносного кода на компьютере пользователя, или убеждает пользователя самостоятельно загрузить и установить вредоносную программу (например, под видом игры или антивирусного средства).

  – «Автоматического метода» – нарушитель осуществляет деструктивное воздействие переадресацию функции автоматического обновления дискредитируемой программы на собственный вредоносный сервер.

- Угроза сбоя обработки специальным образом измененных файлов (УБИ.149) [13]: Угроза заключается в возможности осуществления нарушителем различных неправомерных действий от имени дискредитированных приложений путем вызова сбоя в их работе за счет внесения изменений в обрабатываемые дискредитируемыми программами файлы или их метаданные. Данная угроза обусловлена слабостями механизма проверки целостности обрабатываемых файлов и корректности содержащихся в них данных.

  Реализация данной угрозы возможна в условиях:

  – Наличия у нарушителя сведений о форматах и значениях файлов, вызывающих сбой функционирования дискредитированных приложений при их обработке.

  – Успешно созданном в дискредитируемой системе механизме перехвата управления над обработкой нарушителем программного сбоя.

- Угроза эксплуатации цифровой подписи программного кода (УБИ.162) [14]: Угроза заключается в возможности повышения нарушителем привилегий в системах, использующих цифровую подпись кода в качестве связующей информации между программой и ее привилегиями, путем дискредитации механизма подписывания программного кода. Данная угроза обусловлена слабостями в механизме подписывания программного кода.

  Реализация данной угрозы возможна при следующих условиях:

  − Дискредитируемый программный код написан с помощью фреймворка (*framework*), поддерживающего подписывание программного кода.

  − Дискредитируемый программный код подписан вендором (поставщиком программного обеспечения).

  − Нарушитель имеет возможность внедрить программный код в дискредитируемый компьютер.
- Угроза неправомерного шифрования информации (УБИ.170) [15]: Угроза заключается в возможности фактической потери доступности защищаемых данных из-за их несанкционированного криптографического преобразования нарушителем с помощью известного только ему секретного ключа.

  Данная угроза обусловлена наличием слабостей в антивирусной защите, а также в механизмах разграничения доступа.

  Реализация данной угрозы возможна при условии:

  − Успешной установки нарушителем на дискредитируемый компьютер средства криптографического преобразования информации.

  − Успешного обнаружения (идентификации) нарушителем защищаемых файлов.
- Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью (УБИ.177) [16]: Угроза заключается в возможности возникновения ошибок в работе системы вследствие отсутствия (или игнорирования) процедуры обнаружения и исправления ошибок в данных, вводимых во время работы самим оператором, до активизации управляемого оборудования. Кроме того, к реализации данной угрозы могут привести некорректно реализованные (или отсутствующие) средства реагирования на неправильные, самопроизвольные действия оператора, средства учета нижних/верхних пределов скорости и направления реакции оператора, схемы реагирования на двойное нажатие клавиш при вводе обычных и критических данных, процедуры формирования временных пауз с возможностью выбора разных ответов (да/нет и т.п.).

  Реализуемость данной угрозы зависит от:

  − Требований, предъявляемых к процедурам обнаружения и исправления ошибок во вводимых данных в систему, связанную с безопасностью.

  − Разницы между этими требованиями и фактическим уровнем обнаружения и исправления ошибок.
- Угроза несанкционированной модификации защищаемой информации (УБИ.179) [17]: Угроза заключается в возможности нарушения целостности защищаемой информации путем осуществления нарушителем деструктивного физического воздействия на машинный носитель информации или деструктивного программного воздействия (в т.ч. изменение отдельных бит или полное затирание информации) на данные, хранящиеся на нем.

Реализация данной угрозы возможна в случае получения нарушителем системных прав на запись данных или физического доступа к машинному носителю информации на расстояние, достаточное для оказания эффективного деструктивного воздействия

- Угроза подмены программного обеспечения (УБИ.188) [18]: Угроза заключается в возможности осуществления нарушителем внедрения в систему вредоносного программного обеспечения за счет загрузки и установки вредоносного программного обеспечения, скрытого под видом легитимного свободно распространяемого программного обеспечения. Данная угроза обусловлена наличием у пользователя прав для установки программного обеспечения из сети интернет.

  Реализация данной угрозы возможна:

  – При скачивании программного обеспечения в сети интернет.
- Угроза маскирования действий вредоносного кода (УБИ.189) [19]: Угроза заключается в возможности сокрытия в системе действий вредоносного кода за счет применения специальных механизмов маскирования кода (архивирование, изменение формата данных и др.), которые препятствуют его дальнейшему анализу. Данная угроза обусловлена наличием способов маскирования программного кода, не учтенных сигнатурными базами средств защиты информации, а также механизмов операционной системы, позволяющих осуществить поиск модулей средств защиты информации.

  Реализация данной угрозы возможна при условии:

  – Использования в системе устаревших версий средств защиты информации.
- Угроза внедрения вредоносного кода в дистрибутив программного обеспечения (УБИ.191) [20]: Угроза заключается в возможности осуществления нарушителем заражения системы путем установки недоверенного дистрибутива, в который внедрен вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты.

  Реализация данной угрозы возможна при:

  – Применении пользователем сторонних дистрибутивов.

  – Отсутствии антивирусной проверки перед установкой дистрибутива.
- Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика (УБИ.193) [21]: Угроза заключается в возможности утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика, скрывающих сам факт передачи данных. Данная угроза обусловлена слабостями мер защиты информации при хранении, обработке и передаче информационных ресурсов.

  Реализация данной угрозы возможна:

  – При условии успешного внедрения в дискредитируемую систему указанного вредоносного программного обеспечения.

  – При отсутствии или недостаточной реализации мер межсетевого экранирования.

Помимо понимания сути угрозы, необходимо также установить потенциального злоумышленника для ее реализации, а также объект его воздействия – компонент информационной инфраструктуры предприятия. Соотношение источников и объектов воздействия для приведенных угроз представлено в табл. 1 [6].

Код	Угроза	Источник	Объект
УБИ.111 [7]	Угроза передачи данных по скрытым каналам	Внешний нарушитель со средним потенциалом. Внутренний нарушитель со средним потенциалом.	Сетевой узел. Сетевое программное обеспечение. Сетевой трафик.
УБИ.068 [8]	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Внешний нарушитель со средним потенциалом. Внутренний нарушитель со средним потенциалом.	Системное программное обеспечение. Прикладное программное обеспечение. Сетевое программное обеспечение. Микропрограммное обеспечение. Реестр.
УБИ.069 [9]	Угроза неправомерных действий в каналах связи	Внешний нарушитель с низким потенциалом.	Сетевой трафик
УБИ.088 [10]	Угроза несанкционированного копирования защищаемой информации	Внешний нарушитель с низким потенциалом. Внутренний нарушитель с низким потенциалом.	Объекты файловой системы. Машинный носитель информации.
УБИ.130 [11]	Угроза подмены содержимого сетевых ресурсов	Внешний нарушитель с низким потенциалом.	Прикладное программное обеспечение. Сетевое программное обеспечение, сетевой трафик.
УБИ.145 [12]	Угроза пропуска проверки целостности программного обеспечения	Внешний нарушитель с низким потенциалом. Внутренний нарушитель с низким потенциалом.	Системное программное обеспечение. Прикладное программное обеспечение. Сетевое программное обеспечение.
УБИ.149 [13]	Угроза сбоя обработки специальным образом измененных файлов	Внешний нарушитель со средним потенциалом. Внутренний нарушитель со средним потенциалом.	Метаданные, объекты файловой системы. Системное программное обеспечение.

УБИ.162 [14]	Угроза эксплуатации цифровой подписи программного кода	Внешний нарушитель с низким потенциалом. Внутренний нарушитель с низким потенциалом.	Системное программное обеспечение. Прикладное программное обеспечение.
УБИ.170 [15]	Угроза неправомерного шифрования информации	Внешний нарушитель с низким потенциалом.	Объект файловой системы.
УБИ.177 [16]	Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью	Внутренний нарушитель с низким потенциалом.	Системное программное обеспечение. Сетевое программное обеспечение. Прикладное программное обеспечение. Аппаратное обеспечение.
УБИ.179 [17]	Угроза несанкционированной модификации защищаемой информации	Внешний нарушитель с низким потенциалом. Внутренний нарушитель с низким потенциалом.	Объекты файловой системы.
УБИ.188 [18]	Угроза подмены программного обеспечения	Внутренний нарушитель со средним потенциалом.	Прикладное программное обеспечение. Сетевое программное обеспечение. Системное программное обеспечение.
УБИ.189 [19]	Угроза маскирования действий вредоносного кода	Внешний нарушитель со средним потенциалом.	Системное программное обеспечение. Сетевое программное обеспечение.
УБИ.191 [20]	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Внешний нарушитель с низким потенциалом. Внутренний нарушитель с низким потенциалом.	Прикладное программное обеспечение. Сетевое программное обеспечение. Системное программное обеспечение.

УБИ.193 [21]	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Внешний нарушитель со средним потенциалом.	Информационные ресурсы. Объекты файловой системы.

Реализация атак злоумышленников, происходящая вследствие успешной реализации угроз информационной безопасности, всегда направлена на нарушение одного или нескольких свойств информации: целостности, доступности, конфиденциальности. От результата нарушения данных принципов в случае успешной атаки зависят последствия действий злоумышленника на информацию и инфраструктуру предприятия.

- В результате нарушения целостности информация меняет свой вид, искажается или вовсе перестает существовать.
- В результате нарушения доступности использование информации затрудняется или становится невозможным.
- В результате нарушения конфиденциальности нарушается ее защита, что приводит к ее доступности нелегитимному кругу лиц.

Соотношение угроз в зависимости от влияния на конкретные свойства информации представлено на рис. 1.

Рисунок 1

Таким образом, каждая угроза или атака нарушает хотя бы один принцип информационной безопасности. Также имеются угрозы, затрагивающие все упомянутые принципы, что делает их наиболее опасными и сложными для предотвращения специалистами по информационной безопасности.

Заключение

Таким образом, для обеспечения необходимого и достаточного уровня защиты инфраструктуры от данного вида атак, стоит уделить особое внимание этапу управления рисками информационной безопасности, а именно их установлению, прогнозированию, расчету [22].

Что касается данной работы, то были выделены основные вектора атак злоумышленников, свойственные применению стеганографии:

1. Прямое применение стеганографии в корыстных целях.
2. Использование программных компонентов для сокрытия информации.
3. Использование сетевой стеганографии.
4. Утечки конфиденциальной/критической/корпоративной информацией по скрытым каналам связи.
5. Нарушение работы СЗИ за счет скрытого вложения.

Данные вектора атак были распределены в зависимости от воздействия на принципы информационной безопасности: нарушения целостности, доступности, конфиденциальности информации.

В данной работе были рассмотрены основные угрозы информационной безопасности, наличие которых прямо или косвенно возможно при использовании злоумышленником методов стеганографии при осуществлении атак на информационные инфраструктуры предприятий. Угрозы были выбраны согласно открытому банку данных ФСТЭК России. Для каждой из угроз представлена ее характеристика, выделен потенциальный злоумышленник и объект его воздействия, заключающийся в конкретном компоненте компьютерной инфраструктуры предприятия.

Таким образом, открытая база данных угроз информационной безопасности от ФСТЭК содержит достаточно информации для составления модели нарушителя. Однако этап установления злоумышленника требует более тщательного анализа, заключающегося в его целях, мотивах, инструментах. Данный анализ представлен в работах [3, 23, 24].

Литература

1. URL https://rt-solar.ru/products/solar_dozor/blog/3320/?ysclid=lm6parb5ug278920368 (дата обращения – июль 2024).
2. Коржик В.И., Яковлев В.А. Основы криптографии: учебное пособие – М.: Изд-во Интермедиа, 2017. – 312 с.
3. Федосенко М.Ю., Беззатеев С.В. Анализ проблематики применения методов стеганографии при осуществлении противоправных действий и её роли в цифровой криминалистике // Проблемы информационной безопасности. Компьютерные системы, 2023. – № 3. – С. 33-57.
4. Герлинг Е.Ю., Ахрамеева К.А. Обзор современного программного обеспечения, использующего методы стеганографии // Экономика и качество систем связи, 2019. – № 3. – С. 51-58.

5. URL https://rtmtech.ru/articles/fstek-threats-bank/?ysclid=lsepnzc8q4500547833#anchor2 (дата обращения – июль 2024).
6. URL https://bdu.fstec.ru/threat (дата обращения – июль 2024).
7. URL https://bdu.fstec.ru/threat/ubi.111 (дата обращения – июль 2024).
8. URL https://bdu.fstec.ru/threat/ubi.068 (дата обращения – июль 2024).
9. URL https://bdu.fstec.ru/threat/ubi.069 (дата обращения – июль 2024).
10. URL https://bdu.fstec.ru/threat/ubi.088 (дата обращения – июль 2024).
11. URL https://bdu.fstec.ru/threat/ubi.130 (дата обращения – июль 2024).
12. URL https://bdu.fstec.ru/threat/ubi.145 (дата обращения – июль 2024).
13. URL https://bdu.fstec.ru/threat/ubi.149 (дата обращения – июль 2024).
14. URL https://bdu.fstec.ru/threat/ubi.162 (дата обращения – июль 2024).
15. URL https://bdu.fstec.ru/threat/ubi.170 (дата обращения – июль 2024).
16. URL https://bdu.fstec.ru/threat/ubi.177 (дата обращения – июль 2024).
17. URL https://bdu.fstec.ru/threat/ubi.179 (дата обращения – июль 2024).
18. URL https://bdu.fstec.ru/threat/ubi.188 (дата обращения – июль 2024).
19. URL https://bdu.fstec.ru/threat/ubi.189 (дата обращения – июль 2024).
20. URL https://bdu.fstec.ru/threat/ubi.191 (дата обращения – июль 2024).
21. URL https://bdu.fstec.ru/threat/ubi.193 (Дата обращения – июль 2024).
22. URL https://www.intuit.ru/studies/courses/531/387/lecture/8996?page=1#sect (дата обращения – июль 2024).
23. Ахрамеева К.А., Федосенко М.Ю. Сравнительный анализ возможностей использования стеганографического программного обеспечения для скрытого обмена данными в сети интернет // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки, 2022. – № 1. – С. 37-43.
24. Федосенко М.Ю. Особенности решения задачи управления рисками информационной безопасности при разработке методов защиты от скрытого (стеганографического) обмена информацией на публичных интернет-ресурсах // Проблемы информационной безопасности. Компьютерные системы, 2024. – № 1. – С. 80-95.