УДК 004.73

ВЕРОЯТНОСТНАЯ ОЦЕНКА ПОЯВЛЕНИЯ КИБЕРНЕТИЧЕСКИХ УГРОЗ ПО БЕСПРОВОДНЫМ КАНАЛАМ СВЯЗИ ПРИ ЭКСПЛУАТАЦИИ ВЫСОКОАВТОМАТИЗИРОВАННЫХ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СРЕДСТВ

И.Е.САФОНОВА

Перечислены киберугрозы и принципы информационной безопасности для беспилотных транспортных средств. Представлена разработанная вероятностная модель, позволяющая осуществлять прогностическую оценку появления киберугроз по беспроводным каналам связи.

Ключевые слова: *беспилотные транспортные средства, киберугрозы, беспроводные каналы связи, вероятностная модель, прогностическая оценка, кибербезопасность.*

PROBABILITY ASSESSMENT OF THE APPEARANCE OF CYBERNETIC THREATS OVER WIRELESS COMMUNICATION CHANNELS WHEN OPERATING HIGHLY AUTOMATED UNMANNED VEHICLES

I.E. SAFONOVA

Cyber threats and information security principles for unmanned vehicles are listed. A developed probabilistic model is presented that allows for a predictive assessment of the emergence of cyber threats through wireless communication channels.

Key words: *unmanned vehicles, cyber threats, wireless communication channels, probabilistic model, predictive assessment, cyber security.*

Для беспилотных транспортных средств ключевой задачей является обеспечение высокоскоростного бесперебойного и надежного сетевого подключения, так как даже минимальные задержки передачи информации для высокоавтоматизированного транспорта являются критичными. Эта задача реализуется с помощью технологии 5G (сетей пятого поколения).

Беспилотные транспортные средства используют беспроводные каналы связи и очень уязвимы для различных кибернетических угроз (киберугроз) [1]. Оценка кибернетической безопасности беспилотных транспортных средств – это процесс непрерывный во времени.

Как правило задача обеспечения кибернетической безопасности заключается в создании моделей представления процессов безопасности. Необходимо отметить, что различают следующие основные виды моделей – эвристические, натурные и математические. Выбор модели и обеспечение точности моделирования – эта наиболее важная задача. При этом необходимо помнить, что моделирование предполагает принятие допущений различной степени [2].

С практической точки зрения, применение модели эффективно, если модель отвечает таким требованиям как: универсальность; адекватность; эффективность; точность; наглядность; возможность развития; функционирование в различных условиях, включая условия неопределенности исходной информации и т.д. Результат моделирования зависит от адекватности описательной модели [2]. Эффективность применения модели на практике является интегральной характеристикой. Эффективность модели может быть снижена из-за действия погрешностей среди которых можно выделить:

- информационные ограничения,
- высокая стоимость при реализации на практике,
- не все исходные данные являются достоверными.

С учетом того, что в настоящее время происходит массовое появление беспилотных транспортных средств, развивается и законодательное регулирование их создания/эксплуатации. Например, предложена и утверждена концепция обеспечения безопасности дорожного движения с участием беспилотных транспортных средств, которая разработана на основе Указа Президента РФ от 7 мая 2018 г. N 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» и федерального проекта «Общесистемные меры развития дорожного хозяйства» [3].

В этой Концепции приводится описание различных форм автоматизации транспорта, например - highly automated vehicle, driverless car, unmanned vehicle, fully automated vehicle, self-driving vehicle и других [3]. Используются следующие определения: automated driving system, ADS; ADAS; platooning; dynamic driving task, DDT; интеллектуальная транспортная система - intelligent transport system, ITS; cooperative intelligent transport system, C-ITS на основе технологий V2X; connected vehicle; situational awareness; operational design domain, ODD; Vehicle-to-Vehicle, V2V; Vehicle-to-Infrastructure, V2I; Vehicle-to-Pedestrian, V2P; Vehicle-to-Everything, V2X; C-V2X, Cellular Vehicle-to-Everything; ITS-G5 (европейская группа стандартов ETSI) и т.д.

Системы V2X (технология - Vehicle-to-everything) дают возможность беспилотному транспорту обмениваться информацией по беспроводным каналам связи, например, использование сотовой связи в Cellular-V2X.

Применение технологии VANET (Vehicular Ad-Hoc Network - одноранговые транспортные саморегулирующиеся сети), позволяет беспилотным транспортным средствам взаимодействовать друг с другом через беспроводной канал связи.

В концепции показано, что в настоящее время процессы информатизации транспортных средств достигли очень высокого уровня, приводится описание основных угроз, и в частности киберугроз. На рисунке 1 пунктирными стрелками схематично показаны киберугрозы на беспилотное транспортное средство по беспроводным каналам связи.

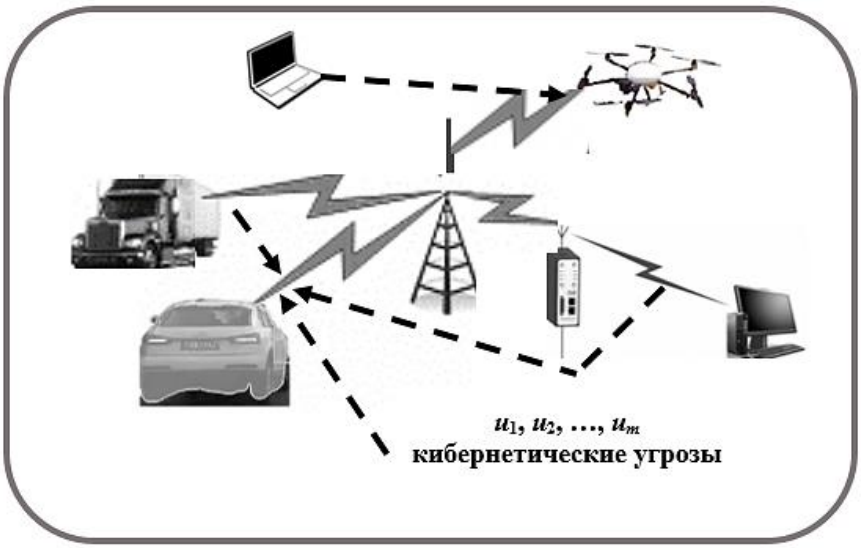

Рисунок 1 – Схематичное представление киберугроз по беспроводным каналам связи

Основные киберугрозы по беспроводным каналам связи, представляющие опасность для высокоавтоматизированных беспилотных транспортных средств [2, 3, 4, 5]:

- взлом беспилотного транспортного средства;

- попытки радиоэлектронного подавления высокоавтоматизированного транспортного средства;
- утечки передаваемой информации и персональных данных участников движения;
- перехват управления транспортным средством, включая перехват управления внутренними системами - антиблокировочной системой торможения, системой управления двигателем;
- атаки, например – GPS Spoofing attack.

Концепция предусматривает реализацию следующих принципов кибернетической безопасности, таких как [3, 5]:

- исключение возможности вмешательства в управление движением;
- отчет о кибербезопасности на основе унифицированных стандартов;
- уведомление водителей о наличии киберугроз для принятия необходимых действий;
- отчетность о неисправностях высокоавтоматизированных транспортных средств и о потенциальных уязвимостях для кибератак;
- мониторинг и обеспечение защиты от киберугроз;
- обеспечение конфиденциальности персональных данных водителей и пользователей транспортных средств;
- защита каналов связи.

С учетом принятой Концепции и для более эффективного мониторинга киберугроз предложена разработанная математическая модель, позволяющая проводить прогностическую оценку появления таких угроз по беспроводным каналам связи в различные моменты времени (вероятностная оценка) [5, 6].

Важным ограничением на применение этой модели является - получение количественных оценок.

Обозначим через T – исследуемый промежуток времени, в течение которого беспилотное транспортное средство может подвергаться киберугрозам (хакерским атакам, взлому, перехвату управления и т.д.) по беспроводным каналам связи – это множество $K = \{K_1, K_2, \dots, K_i, \dots, K_l\}$.

Можно рассмотреть два случая:

1) $T = t$, где t – начальный анализируемый временной промежуток;

2) $T \in [t, t^*]$, где $t^* = t + \Delta t$.

1. *Вероятность поступления киберугроз для первого случая, когда* $T = t$.

Если u случайная величина - появление киберугроз для беспилотного транспортного средства, которая принимает значения $u_1, u_2, \dots, u_m$ с вероятностью $p_1, p_2, \dots, p_m$, тогда математическое ожидание появления угроз на одном из беспроводных каналов связи K_i равно [6]:

$$MO(u) = \sum_{i=1}^{m} p_i u_i. \quad (1)$$

Пусть λ - частота появления киберугроз (статистически определена за время t), тогда ожидаемое число угроз составляет λt. Если разделить временной отрезок t на множество m элементарных, где

$$t = \{t_1, t_2, \dots, t_m\}, \quad (2)$$

то можно считать вероятность появления угроз на таком временном элементарном отрезке равной $\lambda t/m$.

Вероятность того, что киберугрозы не поступят по K_i-каналу на элементарном отрезке равна:

$$1 - \lambda t/m. \quad (3)$$

Вероятность того, что на всех элементарных временных отрезках не поступит ни одной киберугрозы можно определить с помощью выражения:

$$P(t) = \lim_{m\to\infty}\left(1-\frac{\lambda t}{m}\right)^m = e^{-\lambda t}. \quad (4)$$

Далее необходимо вычислить распределение интервала времени t между произвольными двумя соседними событиями (появлением киберугроз).

Вероятность того, что на участке времени длиной *t* после появления одной угрозы больше не появится угроз равна:

$$P\left(t \geq t_j\right) = P(t) = e^{-\lambda t}. \quad (5)$$

Тогда вероятность противоположного события определяется с помощью выражения:

$$\Phi(t) = P\left(t < t_j\right) = 1 - P(t) = 1 - e^{-\lambda t}, \quad (6)$$

где *Ф(t)* - функция распределения для всех *u*.

Плотность вероятности случайной величины есть производная функции распределения *Ф(t)* [6]:

$$\varphi(t) = \Phi'(t) = \lambda e^{-\lambda t} \quad (7)$$

Интервал времени между двумя соседними событиями (появлением киберугроз по исследуемому беспроводному каналу связи K_i) может иметь показательное распределение, следовательно, с учетом выражений (2) – (7) математическое ожидание равно:

$$K_i : MO(u) = 1/\lambda. \quad (8)$$

2. *Вероятность поступления киберугроз по исследуемому беспроводному каналу связи K_i для второго случая, когда $T \in [t, t^*]$.*

Пусть процесс поступления киберугроз по беспроводному каналу связи K_i является нетипичным, а стационарные вероятности числа угроз в момент поступления –

$$a_m = \lim_{t\to\infty} P\{N(t) = m \mid \text{киберугрозы поступают после момента } t\}, \quad (9)$$

необязательно равны соответствующим безусловным стационарным вероятностям:

$$p_m = \lim_{t\to\infty} P\{M(t) = m\}, \;\; p_m = a_m, \; m = 0,1, \ldots, \quad (10)$$

тогда, для любого момента времени и интервала $\Delta t > 0$ число угроз, поступивших в интервале (t, t^*), не зависит от числа угроз уже поступивших до момента *t*. Это предположение справедливо, если интервалы между моментами поступлениями киберугроз по каналу K_i и длительностью момента реагирования на них системой кибербезопасности независимы [5, 6].

Равенство $p_m = a_m$, выполняется, так как, по предположению $\{M(t) = m\}$ – угроза поступила сразу же после момента *t*, независимы. В результате условная вероятность будет равна безусловной.

Пусть $u(t, t^*)$ соответствует событию, что киберугрозы поступают в интервале (t, t^*):

$$p_m(t) = P\{M(t) = m\}, \quad (11)$$

$$a_m = P\{M(t) = m \mid \text{угрозы поступают сразу же после момента } t\}. \quad (12)$$

Согласно формулам (9) – (12), и используя теорему Байеса можно получить, что [6]:

$$a_m = \lim_{\Delta t\to 0} P\{M(t) = m | u(t, t^*)\} =$$

$$= \lim_{\Delta t\to 0} \frac{P\{M(t)=m, u(t,t^*)\}}{P\{u(t,t^*)\}} \lim_{\Delta t\to 0} \frac{P\left\{u(t, t^*)\middle| M(t) = n\right\} P\{M(t)=m\}}{P\{u(t,t^*)\}}. \quad (13)$$

Тогда,

$$P\{u(t, t^*)|M(t) = m\} = P\{u(t, t^*)\}: a_m(t) = P\{M(t) = m\} = p_m(t). \quad (14)$$

Если процесс поступления угроз пуассоновский, то поступившая киберугроза определяется обычным состоянием системы кибербезопасности - $S_B^{\text{cybersecurity}}$.

Вероятность распределения числа угроз, поступающих к беспилотному транспортному средству после реакции системы кибербезопасности на поступившие угрозы по каналу K_i равна:

$$d_m P\{M(t) = m \mid \text{ угрозы поступают в промежуток времени } t^*\}. \quad (15)$$

Их соответствующие стационарные вероятности можно обозначить как

$$d_m = \lim_{t\to\infty} d_m(t)\,, m = 0{,}1, \ldots. \quad (16)$$

Исходя из формул (13) – (16), математическое ожидание равно:

$$K_i : MO(u) = \sum_{j=1}^{m} d_m. \quad (17)$$

При общих предположениях $d_m = a_m, m = 0{,}1, \ldots$ достигается стационарное состояние системы кибербезопасности $S_{ST}^{\text{cybersecurity}}$, в котором стационарные вероятности положительны при всех m, и число киберугроз $M(t)$ имеет приращения, равные 1 (единице) [6]. Для любого состояния системы кибербезопасности от $S_{m-1}^{\text{cybersecurity}}$ до $S_m^{\text{cybersecurity}}$ из-за поступления новой угрозы в дальнейшем будет соответствующее уменьшение от m-1 до m из-за реакции системы на эту угрозу (предотвращение, устранение и т.д.) для каждого канала связи. Следовательно, для длительного промежутка времени доля переходов системы из n в n+1 среди общего их числа равна доле переходов из m-1 в m среди всех имеющихся переходов, а $d_m = a_m$. В стационарном состоянии для поступающих и обработанных (предотвращенных/устраненных) угроз системой кибербезопасности может быть определена как статистически одинаковая для K_i.

В зависимости от полученных результатов можно применять соответствующие методы обеспечения кибербезопасности для беспилотных транспортных средств.

Следует отметить, что особенностями задачи создания систем информационной безопасности и, в частности систем кибербезопасности, для высокоавтоматизированных беспилотных транспортных средств являются:

- неполнота и неопределенность исходной информации об киберугрозах,
- многокритериальность задачи,
- одновременное использование количественных и качественных показателей.

Эти условия и прогностическую вероятностную оценку появления киберугроз по беспроводным каналам связи следует учитывать при проектировании систем кибербезопасности беспилотных транспортных средств.

Необходимо отметить, что в настоящее время уже появляются системы защиты, например, программа «Jarvis», которая предназначена для защиты беспилотных автомобилей от взломов и уязвимостей [7]. Однако, разработанная математическая модель прогностической оценки появления киберугроз по беспроводным каналам связи позволяет снизить риски их реализаций. Эту модель целесообразно использовать: при проектировании систем обеспечения кибербезопасности высокоавтоматизированных транспортных средств, включая защиту беспроводных каналов связи; для проведения предварительного анализа о возможных киберугрозах на стадии разработки беспилотных транспортных средств; для сбора и мониторинга киберугроз.

Литература

1. Основы киберугрозы, типы угроз [сайт]. URL: https://itsecforu.ru (дата обращения: 01.11.2020).

2. Абрамов А.В., Голдовский Я.М., Желенков Б.В., Сафонова И.Е. Постановка задачи разработки и экономическая эффективность проекта «Открытая интегральная цифровая среда обеспечения транспортных перевозок» Инновационные,

информационные и коммуникационные технологии: сборник трудов XVII Международной научно-практической конференции. / под.ред. С.У.Увайсов – Москва: Ассоциация выпускников и сотрудников ВВИА им. проф. Жуковского, 2020, стр.14-18.

3. Концепция обеспечения безопасности дорожного движения с участием беспилотных транспортных средств на автомобильных дорогах общего пользования [сайт]. URL:https://www.garant.ru/products/ipo/prime/doc/73707148 (дата обращения: 06.11.2020).

4. Технологии беспилотного транспорта. [сайт]. URL: https://bespilot.com/tekhnologii (дата обращения: 02.11.2020).

5. Сафонова И.Е., Желенков Б.В., Голдовский Я.М., Панькина К.Е. Архитектура беспилотной транспортной сети. В сборнике: Модели интеграционных решений повышения конкурентоспособности отечественной науки сборник статей Всероссийской научно-практической конференции. Уфа, 2019. С. 39-43.

6. Вентцель Е.С. Теория вероятностей. Учеб. Для вузов. 4-е изд. М.: Наука. 1969. – 575с.

7. BlackBerry «Джарвис» для поиска уязвимостей в беспилотных авто [сайт]. URL: https://republic.ru/posts/88954 (дата обращения: 02.11.2020).