Russian Technological Journal.
2025;13(1):28–37

ISSN 2782-3210 (Print)
ISSN 2500-316X (Online)

Информационные системы. Информатика. Проблемы информационной безопасности

Information systems. Computer sciences. Issues of information security

УДК 519.95:621.3
https://doi.org/10.32362/2500-316X-2025-13-1-28-37
EDN BUGTUV

НАУЧНАЯ СТАТЬЯ

Анализ вероятностных характеристик воздействия вирусных атак на цифровые подстанции

А.С. Леонтьев, Д.В. Жматов @

МИРЭА – Российский технологический университет, Москва, 119454 Россия
@ *Автор для переписки, e-mail: zhmatov@mirea.ru*

Резюме

Цели. Цель данного исследования заключается в создании аналитических методов для оценки вероятностных характеристик безопасности информационных и программных элементов цифровых подстанций. Эти методы направлены на обеспечение кибербезопасности в условиях различных сценариев воздействия вирусов.

Методы. Использованы методы, базирующиеся на теории надежности, теории случайных процессов и теории восстановления.

Результаты. Выведены интегральные соотношения, которые позволяют оценить вероятностные характеристики безопасности обработки информации при выполнении функциональных задач в различных сценариях атак на цифровые подстанции, а также при использовании различных технологий защиты от подобных угроз. Проведены численные исследования вероятности безопасной обработки информации при различной интенсивности атак и времени их активации с учетом частоты проведения диагностики системы обслуживающим персоналом и требований заказчика к безопасному функционированию системы в определенный период времени. Расчеты выполнены для различных технологий защиты от подобных атак на цифровые подстанции. Показано, что технология защиты с детерминированной частотой диагностики системы может обеспечить требования заказчика к безопасности только при случайных и относительно редких вирусных атаках. Технологии защиты, учитывающие различные режимы работы обслуживающего персонала, могут обеспечить выполнение требований заказчика по вероятности безопасной обработки информации в заданный период времени и при преднамеренных атаках на цифровые подстанции.

Выводы. Рассмотренные технологии защиты информации от атак на цифровые подстанции могут обеспечить необходимый уровень безопасности функционирования информационной системы для всех видов угроз при условии увеличения частоты диагностики системы с 2 раз в 1 ч до не реже 1 раза в 25 мин. Это подчеркивает важность активной мониторинговой политики в условиях постоянно меняющейся среды атак для цифровых подстанций.

Ключевые слова: цифровые подстанции, характеристика потоков, вирусы, вероятность безопасного функционирования, информационно-вычислительные системы

• **Поступила:** 12.04.2024 • **Доработана:** 12.09.2024 • **Принята к опубликованию:** 21.11.2024

Для цитирования: Леонтьев А.С., Жматов Д.В. Анализ вероятностных характеристик воздействия вирусных атак на цифровые подстанции. *Russian Technological Journal.* 2025;13(1):28–37. https://doi.org/10.32362/2500-316X-2025-13-1-28-37, https://elibrary.ru/BUGTUV

Прозрачность финансовой деятельности: Авторы не имеют финансовой заинтересованности в представленных материалах или методах.

Авторы заявляют об отсутствии конфликта интересов.

RESEARCH ARTICLE

Probabilistic characteristics analysis of virus attack effect on digital substations

Alexander S. Leontyev, Dmitry V. Zhmatov @

MIREA – Russian Technological University, Moscow, 119454 Russia
@ *Corresponding author, e-mail: zhmatov@mirea.ru*

Abstract

Objectives. This study aims to create analytical methods for evaluating the probabilistic safety characteristics of information and software elements in digital substations in order to ensure security in different virus scenarios.

Methods. The methods of reliability theory, random process theory, and recovery theory were used.

Results. The derived integral ratios were further used to estimate the probability characteristics of information processing security when performing functional tasks in various scenarios of attacks on digital substations, as well as multiple technologies used for protection against such threats. Numerical studies of safe information processing probability of different intensities of attacks and times of their activation were conducted, in order to consider the frequency of diagnostics of the system by the service personnel and customer requirements for the safe operation of the system in a certain period. We performed calculations for various protection technologies against similar attacks on digital substations. A protection technology with system diagnostic deterministic frequency can support customer requirements in the event of accidental and relatively rare virus attacks. Security technologies consider different maintenance personnel operation modes to ensure customer fulfillment requirements for safe information processing probability and the case of deliberate attacks on digital substations in each period.

Conclusions. The technologies considered herein for information protection from attacks on digital substations can provide the necessary level of information security system operation for all types of threats. These technologies can be applied when the system diagnostics frequency increases from twice an hour to at least once every 25 minutes. Our findings underline the importance of timely monitoring of ever-changing attack environments for digital substations.

Keywords: digital substations, flow characteristic, viruses, safe operation probability, information, and computer systems

• **Submitted:** 12.04.2024 • **Revised:** 12.09.2024 • **Accepted:** 21.11.2024

For citation: Leontyev A.S., Zhmatov D.V. Probabilistic characteristics analysis of virus attack effect on digital substations. *Russian Technological Journal.* 2025;13(1):28–37. https://doi.org/10.32362/2500-316X-2025-13-1-28-37, https://elibrary.ru/BUGTUV

Financial disclosure: The authors have no financial or proprietary interest in any material or method mentioned.

The authors declare no conflicts of interest.

ВВЕДЕНИЕ

Современные информационно-вычислительные системы (ИВС) входят в состав контура управления социально-экономическими и общественно-политическими процессами и позволяют автоматизировать основные этапы анализа сложившейся обстановки, выявить возникновение и развитие кризисных ситуаций, формировать рекомендации по их устранению и предотвращению и предоставлять аналитически обработанную и обобщенную информацию должностным лицам для выработки и принятия решений [1]. Поэтому к таким системам предъявляются повышенные требования по своевременности и достоверности обрабатываемой информации.

Программно-технические средства ИВС должны обеспечивать поддержку процессов подготовки документов с учетом возможных помех, включая воздействие вирусов, отказы, сбои, искажение информации [2]. Впервые комплексное использование аналитических методов исследования вирусных угроз и моделирование на их основе процессов воздействия вирусов на информационную систему с помощью инструментально-моделирующего комплекса программ «*КОК*» рассмотрено в базовой работе Костогрызова А.И. и Резникова Г.А. [3]. Для обеспечения возможности совместного использования оригинальных многоуровневых сетевых аналитических моделей исследования ИВС, учитывающих искажения во входной информации [2], и аналитических

моделей, учитывающих искажение информации вирусами, представляется целесообразным расширить класс моделей, рассмотренных в работе [3], с помощью методов теории восстановления, как это было продемонстрировано в работе [4].

Вопросы оценки вероятностно-временных характеристик процессов обработки информации с учетом отказов, сбоев, искажений входной информации при ограничениях на время обслуживания, заданных заказчиком, и оценки характеристик надежности аппаратно-программных средств ИВС и сетей, являющихся источником информации для ситуационных центров, рассмотрены в работах [2, 5, 6]. Отметим, что в настоящее время не уделяется достаточного внимания вопросам оценки воздействия вирусов на вероятностно-временные характеристики обработки информации с учетом требований заказчика к безопасности функционирования системы и с учетом различных технологий защиты информации обслуживающим персоналом. Поэтому задача аналитической оценки вероятностных характеристик безопасности информационных и программных ресурсов при различных сценариях воздействия вирусов и разных технологиях защиты информации является актуальной и обладает новизной.

Исследованию компьютерных вирусов и их влиянию на безопасность данных, основным способам проникновения вирусов в систему, а также сравнительному анализу антивирусных программ посвящены работы [7–11]. В работах [12–15] предложены аналитические модели, позволяющие более точно определить интенсивность вирусных атак. Результаты этих статей являются исходными данными для разработки модели более высокого уровня безопасности функционирования информационных технологий, которая рассматривается в данной работе.

В современном цифровом мире, где информационные технологии играют ключевую роль в управлении различными системами, включая энергетические сети, безопасность данных становится приоритетной задачей. Одним из основных вызовов в этом контексте является защита цифровых подстанций от вредоносных воздействий, таких как вирусы.

Для эффективной защиты цифровых подстанций от вирусов необходимо иметь оценочные модели, которые позволят предсказать вероятностные характеристики возможного воздействия вирусов на систему. Такие модели могут помочь в разработке стратегий защиты и принятии решений о безопасности информационной инфраструктуры.

Одним из ключевых элементов оценочных моделей является учет вероятности воздействия вирусов на цифровые подстанции. Для этого необходимо анализировать различные сценарии атак и оценивать вероятность их возникновения. Кроме того, важно учитывать вероятность обнаружения и удаления вирусов, а также их потенциальные последствия для работы системы.

Учет временных характеристик атак представляет собой еще один значимый аспект. Возможно, вирусы проявляют активность в определенные временные интервалы или действуют непрерывно. Оценочные модели должны учитывать такие временные параметры для правильной оценки рисков и разработки соответствующих контрмер. Также необходимо учитывать различные технологии защиты, которые могут быть применены для предотвращения и обнаружения вирусных атак на цифровые подстанции. Оценочные модели должны учитывать эффективность этих технологий и их способность обеспечивать безопасность системы.

1. ОСНОВНЫЕ КИБЕРАТАКИ НА ЦИФРОВЫЕ ЭЛЕКТРОПОДСТАНЦИИ

Цифровые электроподстанции представляют собой критическую часть современной инфраструктуры, обеспечивая надежную передачу и распределение электроэнергии. Однако с развитием технологий цифровые подстанции становятся более уязвимыми к кибератакам.

В табл. 1 представлен список основных вирусных атак на цифровые электроподстанции.

Тип вирусной атаки может влиять на различные аспекты цифровой электроподстанции, включая:

- *Функциональность системы.* Вирусные атаки могут нарушить нормальное функционирование систем управления, мониторинга и защиты, что приведет к выходу системы из строя или неправильной работе.
- *Безопасность данных*. Некоторые типы вирусов могут направляться на кражу или уничтожение данных, хранящихся на цифровой подстанции, что может привести к утечкам конфиденциальной информации или потере важных данных.
- *Целостность системы*. Вирусные атаки могут нанести ущерб физическому оборудованию или программным компонентам подстанции, что приводит к потере или повреждению оборудования и прерыванию работы.
- *Доступность системы*. Некоторые вирусные атаки могут вызвать отказы в обслуживании или перегрузку сетевых ресурсов, что приводит к временной недоступности системы для обработки запросов операторам.
- *Безопасность персонала*. Вирусные атаки могут создавать опасные ситуации для персонала, работающего на подстанции, например, путем изменения параметров системы без их ведома или возможного вызова физического повреждения оборудования.

Таблица 1. Вирусные атаки на цифровую электроподстанцию

Название атаки	Описание	Потенциальные последствия
SQL-инъекция	Внедрение злонамеренного SQL-кода в приложение или базу данных через некорректную обработку пользовательского ввода	Получение несанкционированного доступа к данным, изменение или удаление информации в базе данных
Вредоносное программное обеспечение	Установка вредоносного программного обеспечения на компьютеры или устройства подстанции с целью кражи данных, прерывания работы или управления системой	Нарушение работы подстанции, потеря конфиденциальности данных, прерывание электроснабжения
Фишинг	Отправка поддельных электронных сообщений с целью обмана персонала подстанции для получения доступа к системам или конфиденциальной информации	Несанкционированный доступ к системам, утечка конфиденциальных данных
DDos-атака[1]	Перегрузка сети или серверов подстанции путем отправки большого количества запросов с целью нарушения работы	Отказ в обслуживании, временное или длительное прерывание работы подстанции
Подмена GOOSE-сообщений[2]	Получение несанкционированного доступа к системам подстанции путем использования украденных учетных данных	Потенциальное изменение параметров работы системы, нарушение ее работы, угроза безопасности электроснабжения
Ransomware (программа-вымогатель)	Заражение системы вредоносным программным кодом, блокировка доступа к данным, требование выкупа для их восстановления	Потеря данных, прерывание работы подстанции, финансовые убытки
Man-in-the-Middle (атака посредника)	Перехват и изменение коммуникаций между устройствами подстанции, чтобы злоумышленник мог манипулировать данными	Возможность управления и искажения данных, прерывание обмена информацией
Zero-Day Exploit (атака нулевого дня)	Использование уязвимости в программном обеспечении, которая еще не была обнаружена и устранена разработчиками	Несанкционированный доступ, внедрение вредоносного кода, потенциальная угроза безопасности системы
Спуфинг (фальсификация)	Подделка адресов или идентификационных данных, чтобы создать ложное восприятие подлинности или авторизации	Нарушение аутентификации, возможное введение в заблуждение системы управления
Атака на физические устройства	Попытка воздействия на физические компоненты подстанции, такие как силовые трансформаторы или выключатели	Потенциальные повреждения оборудования, прерывание электроснабжения

- *Финансовые потери*. В случае успешной вирусной атаки могут возникнуть значительные финансовые потери, связанные с восстановлением системы, упущенным доходом из-за простоя оборудования и компенсацией ущерба потребителям.

Угрозы со стороны внутренних пользователей, таких как сотрудники энергетических компаний, также представляют серьезную опасность для безопасности цифровых подстанций. Несанкционированный доступ к системам, утеря конфиденциальной информации или злонамеренные действия внутри самой компании могут привести к катастрофическим последствиям.

Меры по предотвращению потенциальных последствий вирусных атак:

- регулярное обновление программного обеспечения и систем защиты;
- внедрение многоуровневой аутентификации для доступа к системам управления подстанциями;
- обучение персонала основам кибербезопасности и идентификации фишинговых атак;
- мониторинг сетевой активности для выявления подозрительного поведения;
- реализация четких политик безопасности и контроля доступа к критическим системам.

[1] Distributed denial of service – распределенный отказ в обслуживании. [Distributed denial of service.]

[2] Generic object-oriented substation event – протокол, который предназначен для связи между устройствами релейной защиты посредством передачи данных в цифровом виде по Ethernet. [Generic object-oriented substation event is a protocol designed for communication between relay protection devices by transmitting data digitally over Ethernet.]

Кибератаки на цифровые электроподстанции представляют серьезную угрозу для энергетической инфраструктуры. Понимание основных видов атак и принятие соответствующих мер по их предотвращению является важной задачей для обеспечения безопасности и надежности работы подстанций в условиях возрастающего числа киберугроз.

2. ПОСТАНОВКА И РЕШЕНИЕ ЗАДАЧИ ОЦЕНКИ ВЕРОЯТНОСТНЫХ ХАРАКТЕРИСТИК БЕЗОПАСНОСТИ ДЛЯ ЦИФРОВЫХ ПОДСТАНЦИЙ

Предполагается, что используемые средства профилактической диагностики позволяют выявить все проникшие вирусы и следы их воздействия, а средства восстановления способны полностью восстановить нарушенную целостность информационных и программных ресурсов i-го типа. В результате диагностики вирусы ликвидируются, при обнаружении искажений восстанавливается целостность информационных и программных ресурсов, обработка прерванных запросов повторяется заново после восстановления целостности системы.

Оценка с использованием аналитических подходов основана на применении методов теории восстановления случайных процессов [4].

Для проведения необходимых аналитических преобразований необходимо задать:

$V_{\text{возд}}(t)$ – функцию распределения (ФР) времени между воздействиями вирусов на систему;

$V_{\text{акт}}(t)$ – ФР времени активизации вируса после его проникновения в систему;

$F_{\text{диаг}}(t)$ – ФР времени между диагностиками;

$G_i(t)$ – ФР времени обработки информации i-го типа, включающего время ожидания в очереди и непосредственно время обработки.

Используемые функции распределения в рамках теории второго порядка по математическим ожиданиям и дисперсии аппроксимируются в аналитических моделях двухпараметрическими эрланговскими или гиперэкспоненциальными ФР [4].

Моменты ФР $G_i(t)$ (математическое ожидание и дисперсия) оцениваются с помощью многоуровневых моделей, описывающих процессы обработки информации в системе цифровых подстанций. Данные модели формализуются в виде многоуровневых аналитических вложенных моделей (сетей массового обслуживания), с помощью которых формализуются технологические операции обработки с учетом возникающих отказов аппаратных и программных средств [2]. Оригинальность данного подхода связана с тем, что временные характеристики обработки заявок во вложенных сетевых моделях аппаратного уровня слабо зависят от вида ФР, характеризующих потоки заявок на этом уровне, а также от вида потоков в сетевой модели программного уровня. Это позволяет аппроксимировать потоки на аппаратном уровне пуассоновскими потоками и провести не только декомпозицию сетевой модели аппаратного уровня, но и декомпозировать многоуровневую модель на сетевые модели различных уровней, которые исследуются аналитическими методами. В частности, модель аппаратного уровня анализируется с помощью аналитических методов промежуточной теории массового обслуживания, а сетевая модель программного уровня, используя по двум первым моментам аппроксимацию реальных распределений эрланговскими и гиперэкспоненциальными распределениями с помощью метода этапов Эрланга, сводится к эквивалентной марковской, которая анализируется известными аналитическими методами.

Рассмотрим процесс восстановления, в котором точки регенерации соответствуют времени начала очередной антивирусной диагностики цифровых подстанций.

Пусть $\{t_n\}_{n=1}^{\infty}$ – процесс восстановления, моменты t_n которого соответствуют времени проведения очередной антивирусной диагностики системы.

Если интервалы между диагностиками τ одинаковые, то справедлива формула:

$$\xi_i(t) = \int_0^{t_{n+1}-t} V_{\text{возд}}(t - t_n - \theta) V_{\text{акт}}(\theta) dG_i(\theta), \qquad (1)$$

где $\xi_i(t)$ – вероятность того, что во время обработки заявки i-го типа произойдет заражение обрабатываемой информации вирусами на интервале времени $t_n \le t \le t_{n+1}$, $n \ge 1$.

В соответствии с основными свойствами процессов восстановления и предельной теоремой теории восстановления вероятность искажения информации вирусами $P_{\text{vir}(i)}$ определяется соотношением (2), а вероятность того, что информация не искажена, оценивается формулой (3):

$$P_{\text{vir}(i)} = \frac{1}{F^{(1)}_{\text{диаг}}} \int_0^{\infty} \left\{ \left[1 - F_{\text{диаг}}(t)\right] \int_0^{\tau - t} V_{\text{возд}}(t - \theta) V_{\text{акт}}(\theta) dG_i(\theta) \right\} dt, \qquad (2)$$

$$P_{\text{возд}(i)} = 1 - P_{\text{vir}(i)}. \qquad (3)$$

В течение заданного периода времени $T_{\text{зад}}$ от момента последней профилактики при условии $T_{\text{зад}} < F^{(1)}_{\text{диаг}}$, вероятность отсутствия опасного воздействия определяется соотношением:

$$P_{\text{возд}(i)}(T_{\text{зад}}) = 1 - \int_0^{T_{\text{зад}}} V_{\text{возд}}(T_{\text{зад}} - \theta) V_{\text{акт}}(\theta) d\theta. \qquad (4)$$

Отметим, что формула (4) может использоваться и для оценки вероятности отсутствия опасных воздействий без какой-либо диагностики в предположении, что к началу периода $T_{зад}$ целостность информационных ресурсов обеспечена.

3. ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ ОПАСНЫХ ВОЗДЕЙСТВИЙ

При реализации информационных технологий на цифровых электроподстанциях частота проведения регламентных диагностик обслуживающим персоналом существенным образом зависит от частоты воздействия источников опасности, например, вирусов. При проведении расчетов будем рассматривать различные сценарии воздействия угроз (вирусов) на цифровые подстанции и различные сценарии проведения регламентных диагностик обслуживающим персоналом. Из-за недостаточного объема статистики по воздействию вирусов на цифровые подстанции будем считать, что на различных цифровых подстанциях используются одинаковые технологии защиты от вирусных воздействий.

При реализации технологий защиты предполагают, что через определенные промежутки времени осуществляется регламентная диагностика, т.е. системный контроль целостности информационных и программных ресурсов. Полагается, что в случае обнаружения неактивизировавшихся источников опасности (вирусов) или следов их воздействия происходит восстановление целостности системы предусмотренными для этого способами.

Проведем численное исследование вероятности безопасной обработки информации при различной интенсивности воздействия вирусов и времени их активации, разной частоте проведения диагностики системы обслуживающим персоналом и заданных требованиях заказчика по вероятности безопасного функционирования системы.

При расчетах используются следующие обозначения для исходных данных:

j – индекс варианта сценария и метода защиты;

$\sigma_j = \dfrac{1}{V^{(1)}_{возд}}$ – частота воздействия на систему для внедрения вируса;

$\beta_j = F^{(1)}_{акт}$ – среднее время активации проникшего в систему вируса при j-м сценарии;

$T_{меж.\,j} = F^{(1)}_{диаг.\,j}$ – средний интервал времени между окончанием предыдущей диагностики и началом следующей при j-м сценарии;

$T_{диаг.\,j}$ – длительность диагностики, включая восстановление целостности системы (задано заранее).

Пусть заказчик выдвигает требования по следующим параметрам:

$P_{зад.\,j}$ – минимально допустимая вероятность безопасного функционирования системы (задано заранее заказчиком).

Оцениваются следующие показатели:

$P_{возд.\,j}$ – вероятность отсутствия опасного воздействия в течение определенного периода $T_{зад.\,j}$ при j-м сценарии.

С точки зрения пользователя функционирование системы полагается безопасным в течение заданного времени $T_{зад}$ = 1 суткам, если в течение этого времени не состоится ни одного опасного воздействия или же если все источники опасности выявляются сразу при их проникновении в систему. Более того, реализованные модели предполагают, что после диагностики, а также после восстановления целостности система находится в полностью безопасном состоянии.

Среднее время, требуемое для проведения диагностической процедуры, включая ремонтные работы, оценивается в 60 с. Начальные данные для расчетов представлены в табл. 2.

Учитывая недостаточный объем статистики по воздействию вирусов на цифровые подстанции, сценарии воздействия вирусов, включая интенсивность воздействия вирусов и время их активации, выбирались в соответствии с данными, представленными в работе [3], а оценочные расчеты проводились при экспоненциальных функциях распределения. В этом асимптотическом случае аналитические соотношения, полученные с использованием методов теории восстановления, и аналитические формулы, представленные в работе [3], дают одинаковые результаты. Поэтому, как и в работе [3], при проведении предварительных оценочных расчетов воздействия вирусов на электрические подстанции использовался инструментально-моделирующий комплекс для оценки качества функционирования информационных систем «*КОК*». В дальнейшем, также как и в работе [4], реальные распределения будут аппроксимироваться по первым двум моментам двухпараметрическими эрланговскими или гиперэкспоненциальными распределениями.

На рис. 1 представлены результаты расчета вероятности безопасного функционирования цифровых подстанций при различных сценариях воздействия угроз и различных сценариях проведения регламентных диагностик целостности информационных и программных ресурсов обслуживающим персоналом $(j = \overline{1,10})$ в соответствии с заданными исходными данными (табл. 2).

На основании приведенного предварительного оценочного расчета и данных, представленных в табл. 2, можно сделать следующие выводы.

Таблица 2. Оценки безопасности функционирования информационной системы на цифровой подстанции

Характеристики угроз			Характеристики обслуживающего прибора подстанции			Требования заказчика
j	σ_j	β_j	$T_{\text{меж}.j}$	$T_{\text{диаг}.j}$	$T_{\text{зад}.j}$	$P_{\text{зад}.j}$
1	1 нед $^{-1}$	6 ч	1 нед	1 мин	1 сут	0.95
2	1 нед$^{-1}$	6 ч	3 сут	1 мин	1 сут	0.95
3	1 нед$^{-1}$	6 ч	1 сут	1 мин	1 сут	0.95
4	1 нед$^{-1}$	6 ч	6 ч	1 мин	1 сут	0.95
5	1 нед$^{-1}$	6 ч	3 ч	1 мин	1 сут	0.95
6	1 сут$^{-1}$	3 ч	1 сут	1 мин	1 сут	0.90
7	1 сут$^{-1}$	3 ч	6 ч	1 мин	1 сут	0.90
8	1 сут$^{-1}$	3 ч	3 ч	1 мин	1 сут	0.90
9	1 сут$^{-1}$	3 ч	1 ч	1 мин	1 сут	0.90
10	1 ч$^{-1}$	1 ч	30 мин	1 мин	1 сут	0.90

1. Защищенность цифровых подстанций от преднамеренных угроз с частотой воздействия 1 раз в сутки обеспечивается за счет диагностики информационных и программных ресурсов не реже, чем 1 раз в 6 ч (рис. 4, j = 7, 8, 9).
2. Вместе с тем, для угроз, возникающих в среднем 1 раз в 1 ч, вероятность отсутствия опасного воздействия вирусов в течение суток составит 0.88 при частоте диагностики 1 раз в 30 мин, что меньше задаваемых 0.9.

Проведем исследования, позволяющие ответить на вопрос, когда режимы диагностики информационных и программных ресурсов цифровых подстанций способны обеспечить требуемую безопасность цифровых подстанций для наиболее опасного сценария вирусных атак, при котором новые вирусы проникают в систему в среднем 1 раз в 1 ч и время их активации также равно 1 ч.

На рис. 2–5 показаны зависимости вероятности отсутствия опасных воздействий на информационные ресурсы цифровых подстанций для наиболее опасного сценария преднамеренных воздействий вирусов $P_{\text{возд}.10}$ (j = 10) при изменении интенсивности воздействия угроз, среднего времени активации вирусов, интервала между диагностиками и вероятностно-временных требований заказчика.

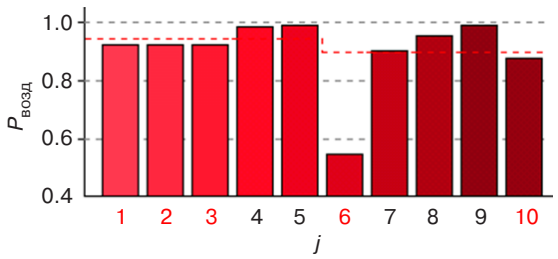

Рис. 1. Вероятность безопасного функционирования информационной системы при различных сценариях воздействия угроз ($j = \overline{1,10}$) для цифровой подстанции

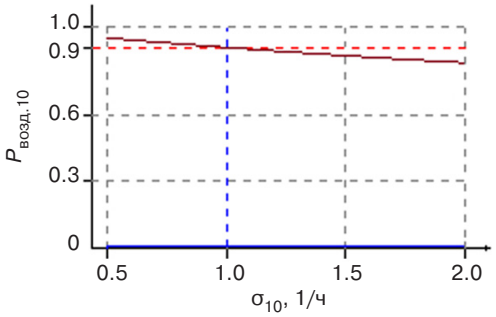

Рис. 2. Зависимость величины $P_{\text{возд}.10}$ от частоты воздействия угроз

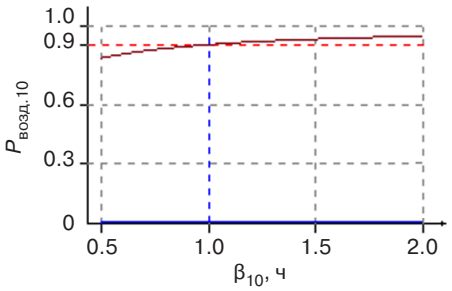

Рис. 3. Зависимость величины $P_{\text{возд}.10}$ от среднего времени активации угрозы

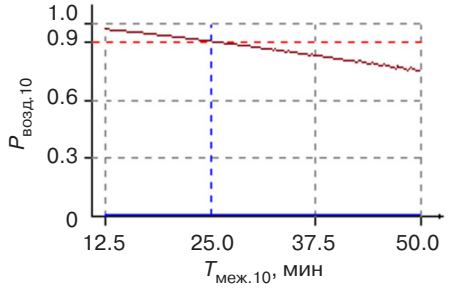

Рис. 4. Зависимость величины $P_{\text{возд}.10}$ от среднего интервала между диагностиками

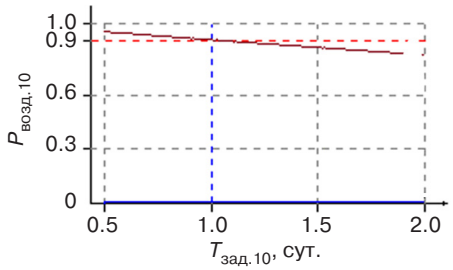

Рис. 5. Зависимость величины $P_{возд.10}$ от заданного заказчиком времени $T_{зад.10}$

Результаты расчетов, представленные на рис. 2–5, показывают, что при увеличении интенсивности вирусных воздействий заметно уменьшается защищенность системы. При увеличении времени активации вирусов увеличивается защищенность системы при всех рассмотренных сценариях. При уменьшении заданного заказчиком времени отсутствия вирусных воздействий $T_{зад}$ увеличивается защищенность системы при всех сценариях угроз и способах защиты.

Как видно из представленных оценочных результатов, защита цифровых подстанций от наиболее опасных сценариев воздействия вирусов при удовлетворении заданных требований заказчика по вероятности безопасного функционирования способна обеспечить требуемую безопасность информационных ресурсов цифровых подстанций, если реализовать диагностику системы не 1 раз в 1 ч, а не реже 1 раза в 25 мин (показано на рис. 4).

Рассмотренные сценарии вирусных угроз и способов борьбы с ними носят общий характер и могут быть применены для исследования защищенности различных цифровых подстанций.

ЗАКЛЮЧЕНИЕ

Приведен обзор основных видов кибератак на цифровые электроподстанции, их потенциальных последствий и мер по их предотвращению.

При проведении исследования получены интегральные соотношения, которые позволяют оценить вероятностные характеристики безопасной обработки информации цифровых подстанций в условиях различных сценариев воздействия вирусов, а также при использовании различной технологий защиты информации от опасных воздействий. Эти соотношения предоставляют возможность провести анализ вероятности безопасной обработки информации цифровых подстанций при различных интенсивности воздействия вирусов, времени их активации, частоте проведения диагностики обслуживающим персоналом и заданных требованиях заказчика по вероятности безопасного функционирования системы управления сообщениями на цифровых подстанциях.

Расчеты выполнены для различных технологий защиты информации цифровых подстанций от опасных воздействий. Особое внимание уделено наиболее опасным сценариям воздействия вирусов и технологии защиты, которая обеспечивает заданную заказчиком безопасность функционирования цифровых подстанций в условиях всех рассмотренных угроз. Важным выводом является то, что при реализации данной технологии и уменьшении интервала проведения диагностики информационных ресурсов цифровых подстанций до 25 мин можно значительно повысить уровень безопасности функционирования системы цифровых подстанций.

Результаты исследования предоставляют практически применимые рекомендации для обеспечения безопасности информационных ресурсов цифровых подстанций при использовании современных технологий защиты от вирусных атак. Сделанные выводы актуальны в контексте растущей сложности угроз и высокой динамики развития цифровых технологий, что подчеркивает необходимость эффективных мер по обеспечению безопасности информационных систем цифровых подстанций.

Вклад авторов

А.С. Леонтьев – разработал интегральные соотношения, позволяющие оценивать вероятностные характеристики безопасности обработки информации; провел численные исследования вероятности безопасной обработки информации при различной интенсивности атак, времени их активации и частоте диагностики системы; проанализировал влияние детерминированной частоты диагностики системы на выполнение требований заказчика по безопасности при случайных и редких атаках.

Д.В. Жматов – исследовал эффективность различных технологий защиты от атак на цифровые подстанции; провел анализ технологий, учитывающих режимы работы обслуживающего персонала, и их влияние на выполнение требований заказчика; сформулировал выводы о необходимости увеличения частоты диагностики системы для обеспечения безопасности при преднамеренных атаках; подчеркнул значение активной мониторинговой политики в условиях изменяющейся среды атак.

Authors' contributions

A.S. Leontyev – developed integral equations to assess the probabilistic characteristics of information processing security; conducted numerical studies on the probability of secure information processing under varying attack intensities, activation times, and system diagnostic frequencies; analyzed the impact of a deterministic diagnostic frequency on meeting customer safety requirements under random and infrequent attacks.

D.V. Zhmatov – investigated the effectiveness of various protection technologies against attacks on digital substations; analyzed protection technologies that consider the operating modes of maintenance personnel and their impact on meeting customer requirements; formulated conclusions about the need to increase system diagnostic frequency to ensure security under deliberate attacks; emphasized the importance of an active monitoring policy in the changing threat landscape for digital substations.

СПИСОК ЛИТЕРАТУРЫ

1. Старовойтов А.В., Стариков П.П., Дубицкий К.А., Лукьянов С.Э., Павлов Л.П., Симонов В.М., Съедин Д.Ю. Комплекс автоматизированных государственных информационных систем поддержки управленческих решений в сфере науки и техники. *Информатизация и связь*. 2021;6:7–19. https://doi.org/10.34219/2078-8320-2021-12-6-7-19
2. Леонтьев А.С. Многоуровневые аналитические и аналитико-имитационные модели оценки вероятностно-временных характеристик многомашинных вычислительных комплексов с учетом надежности. *Международный научно-исследовательский журнал.* 2023;5(131). https://doi.org/10.23670/IRJ.2023.131.8
3. Костогрызов А.И., Резников Г.Я. Моделирование процессов опасного воздействия на защищаемую информационную систему. *Информационные технологии в проектировании и производстве*. 2004;2:17–27.
4. Гусев К.В., Леонтьев А.С. Теоретическое развитие моделей для оценки защищенности от несанкционированного доступа и сохранения конфиденциальности используемой информации. *ИТ Стандарт*. 2021;4(29):38–44.
5. Акимова Г.П., Соловьев А.В., Тарханов И.А. Моделирование надежности распределенных вычислительных систем. *Информационные технологии и вычислительные системы* (*ИТиВС*). 2019;3:70–86. https://doi.org/10.14357/20718632190307
6. Павский В.А., Павский К.В. Математическая модель для расчета показателей надежности масштабируемых вычислительных систем с учетом времени переключения. *Известия ЮФУ. Технические науки*. 2020;2(212):134–145. https://doi.org/10.18522/2311-3103-2020-2-134-145
7. Минитаева А.М., Соколов А.В. Основные способы проникновения и воздействия файловых вирусов на систему. *Международный журнал гуманитарных и естественных наук*. 2023;4–3(79):56–60. https://doi.org/10.24412/2500-1000-2023-4-3-56-60
8. Литвинов П.В. Имитационное моделирование вопросов информационной безопасности как инструмент оценки защищенности и оптимизации затрат. *Мир компьютерной автоматизации.* 2016;1:43–53.
9. Блазуцкая Е.Ю., Шарафутдинов А.Г. Вирусы нового поколения и антивирусы. *NovaInfo.ru*. 2015;1(35):92–94.
10. Попов И.О., Марунько А.С., Петров О.И., Олейник А.А. Вирусы и антивирусные программы в информационной безопасности. *Научные записки молодых исследователей.* 2020;8(4):74–80.
11. Сиденко Г.А., Редько Г.В., Безнос О.С. Сравнительный анализ антивирусных программ. *Научно-образовательный журнал для студентов и преподавателей «StudNet»*. 2020;9:676–680.
12. Заводцев И.А., Борисов М.А., Бондаренко М.М., Мелешко В.А. Уточненный способ аналитического моделирования процессов распространения вирусного программного обеспечения для оценки защищенности объектов информатизации. *Computational nanotechnology*. 2022;9(1):11–20.
13. Бойко А.А. Способ аналитического моделирования процесса распространения вирусов в компьютерных сетях различной структуры. *Труды СПИИРАН*. 2015;5(42):196–211. https://doi.org/10.15622/sp.42.4
14. Магазев А.А., Цырульник В.Ф. Исследование одной марковской модели угроз безопасности компьютерных систем. *Моделирование и анализ информационных систем*. 2017;24(4):445–458. https://doi.org/10.18255/1818-1015-2017-4-445-458
15. Котенко И.В., Воронцов В.В. Аналитические модели распространения сетевых червей. *Труды СПИИРАН*. 2007;4:208–224. https://doi.org/10.15622/sp.4.15

REFERENCES

1. Starovoitov A.V., Starikov P.P., Dubitsky K.A., Lukyanov S.E., Pavlov L.P., Simonov V.M., Syedin D.Yu. Computerized complex of federal information systems for supporting decision-making in the field of science and technology. *Informatizatsiya i svyaz' = Informatization and Communication*. 2021;6:7–19 (in Russ.). https://doi.org/10.34219/2078-8320-2021-12-6-7-19
2. Leontyev A.S. Multilevel Analytical and Analytical-Simulation Models for Evaluating the Probabilistic and Temporal Characteristics of Multimachine Computing Complexes with Regard to Reliability. *Mezhdunarodnyi nauchno-issledovatel'skii zhurnal = International Research Journal*. 2023;5(131) (in Russ.). https://doi.org/10.23670/IRJ.2023.131.8
3. Kostogryzov A.I., Reznikov G.Y. Modeling of Hazardous Impact Processes on Protected Information System. *Informatsionnye tekhnologii v proektirovanii i proizvodstve = Information Technologies in Design and Production*. 2004;2:17–27 (in Russ.).
4. Gusev K.V., Leontiev A.S. Theoretical Development of Models for the Assessment of Security against Unauthorized Access and Preservation of the Confidentiality of the Information Used. *IT Standard*. 2021;4(29):38–44 (in Russ.).
5. Akimova G.P., Solovyev A.V., Tarkhanov I.A. Modeling the reliability of distributed information systems. *Informatsionnye tekhnologii i vychislitel'nye sistemy = Journal of Information Technologies and Computing Systems*. 2019;3:70–86 (in Russ.). https://doi.org/10.14357/20718632190307
6. Pavsky V.A., Pavsky K.V. Mathematical Model for Calculating Reliability Indicators of Scalable Computer Systems Considering Switching Time. *Izvestiya YuFU. Tekhnicheskie nauki = Izvestiya SFedU. Engineering Sciences*. 2020;2(212):134–145 (in Russ.). https://doi.org/10.18522/2311-3103-2020-2-134-145
7. Minitaeva A.M., Sokolov A.V. Main Ways of Penetration and Impact of File Viruses on the System. *Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk = International Journal of Humanities and Natural Sciences*. 2023;4–3(79):56–60 (in Russ.). https://doi.org/10.24412/2500-1000-2023-4-3-56-60

8. Litvinov P.V. Simulation modeling of information security issues as a tool for assessing security and cost optimization. *Mir komp'yuternoi avtomatizatsii = Computer Automation World*. 2016;1:43–53 (in Russ.).
9. Blazutskaya E.Y., Sharafutdinov A.G. Next Generation Viruses and Antiviruses. *NovaInfo.ru*. 2015;1(35):92–94 (in Russ.).
10. Popov I.O., Marunko A.S., Petrov O.I., Oleinik A.A. Viruses and Antivirus Programs in Information Security. *Nauchnye zapiski molodykh issledovatelei = Scientific Notes of Young Scientists*. 2020;8(4):74–80 (in Russ.).
11. Sidenko G.A., Redko G.V., Beznos O.S. Comparative Analysis of Antivirus Programs. *StudNet*. 2020;9:676–680 (in Russ.).
12. Zavodtsev I.A., Borisov M.A., Bondarenko M.M., Meleshko V.A. Refined Method of Analytical Modeling of Viral Software Propagation Processes for Assessing Security of Informatization Objects. *Computational Nanotechnology*. 2022;9(1):11–20 (in Russ.).
13. Boyko A.A. Method of Analytical Modeling of Viruses Propagation Process in Computer Networks with Different Topology. *Trudy SPIIRAN = SPIIRAS Proceedings*. 2015;5(42):196–211 (in Russ.). https://doi.org/10.15622/sp.42.4
14. Magazev A.A., Tsyrulnik V.F. Investigation of a Markov Model for Computer System Security Threats. *Aut. Control Comp. Sci.* 2018;52(7):615–624. https://doi.org/10.3103/S0146411618070180
[Original Russian Text: Magazev A.A., Tsyrulnik V.F. Investigation of a Markov Model for Computer System Security Threats. *Modelirovanie i analiz informatsionnykh sistem*. 2017;24(4):445–458 (in Russ.). https://doi.org/10.18255/1818-1015-2017-4-445-458]
15. Kotenko I.V., Vorontsov V.V. Analytical Models of Network Worms Propagation. *Trudy SPIIRAN = SPIIRAS Proceedings.* 2007;4:208–224 (in Russ.). https://doi.org/10.15622/sp.4.15

Об авторах

Леонтьев Александр Савельевич, к.т.н., старший научный сотрудник, доцент кафедры математического обеспечения и стандартизации информационных технологий, Институт информационных технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: leontev@mirea.ru. SPIN-код РИНЦ 5798-9721, https://orcid.org/0000-0003-3673-2468

Жматов Дмитрий Владимирович, к.т.н., доцент, доцент кафедры математического обеспечения и стандартизации информационных технологий, Институт информационных технологий ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: zhmatov@mirea.ru. Scopus Author ID 56825948100, SPIN-код РИНЦ 2641-6783, https://orcid.org/0000-0002-7192-2446

About the authors

Alexander S. Leontyev, Cand. Sci. (Eng.), Senior Researcher, Associate Professor, Department of Mathematical Support and Standardization, Institute of Information Technologies MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: leontev@mirea.ru. RSCI SPIN-code 5798-9721, https://orcid.org/0000-0003-3673-2468

Dmitry V. Zhmatov, Cand. Sci. (Eng.), Associate Professor, Department of Mathematical Support and Standardization, Institute of Information Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: zhmatov@mirea.ru. Scopus Author ID 56825948100, RSCI SPIN-code 2641-6783, https://orcid.org/0000-0002-7192-2446