www.volsu.ru

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
В БЕЗОПАСНОСТИ И ТЕЛЕКОММУНИКАЦИЯХ

CC BY

DOI: https://doi.org/10.15688/NBIT.jvolsu.2025.2.1

УДК 004.056.5
ББК 32.972.53

# АНАЛИЗ УГРОЗ И УЯЗВИМОСТЕЙ В ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

**Владислав Георгиевич Яриков**

Кандидат педагогических наук,
доцент кафедры методики преподавания математики и физики, ИКТ,
Волгоградский государственный социально-педагогический университет
yarikov_vg@mail.ru
просп. им. Ленина, 27, 400005 г. Волгоград, Российская Федерация

**Александра Николаевна Панченко**

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
IBm-241_744165@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

**Аннотация.** В статье рассматриваются проблемы в области информационной безопасности, связанные с ростом цифровизации и увеличением числа киберугроз. Проанализированы ключевые аспекты защиты информационных систем, включая классификацию угроз, уровни защиты и методологии анализа (OCTAVE, EBIOS, STRIDE). Особое внимание уделено современным типам атак – вирусам, DoS/DDoS и Advanced Persistent Threats (APT).

**Ключевые слова:** кибербезопасность, анализ угроз, уязвимости, OCTAVE, EBIOS, STRIDE, DoS/DDoS, Advanced Persistent Threats.

© Яриков В.Г., Панченко А.Н., 2025

## Введение

В современном мире в условиях постоянного развития технологий потребность использования информационных систем во всех сферах жизни постоянно растет. Однако с увеличением цифровизации возрастает количество киберугроз, а следовательно, и необходимость обеспечения безопасности данных. Своевременный анализ угроз и уязвимостей

позволит снизить риски возможных опасностей, и повысить уровень надежности информационных систем.

Определение основных терминов, используемых в статье:

Информационная система (далее – ИС): совокупность различных средств и методов для сбора, хранения, обработки и передачи информации.

Защищенность информационной системы: степень устойчивости системы к воздействиям различных угроз, направленных на нарушение целостности и конфиденциальности информации.

## Классификация информационных систем и уровней их защиты

Для обеспечения надежной защиты ИС используется комплекс мер, позволяющий создать многоуровневую систему безопасности. Выделяются следующие уровни:

1. Физический уровень: с помощью контроля доступа, видеонаблюдения и т. д. обеспечивает защиту аппаратного обеспечения и серверных помещений.

2. Уровень сетевой защиты отвечает за угрозы ИС, связанные с кибератаками.

3. Прикладной уровень обеспечивает безопасность прикладных программных продуктов. Для этого используются аутентификация и авторизация, а также криптографические методы, например, шифрование данных.

4. На организационном уровне проводятся разработка и внедрение политик информационной безопасности.

Классифицировать информационные системы можно по характеру использования, лицензированию и модели эксплуатации. Виды таких ИС:

1) тиражируемые (адаптированные) информационные системы: формируются на основе использования стандартного функционала, с последующими небольшими доработками, нужными для конкретных целей компании [2]. Обычно данные системы эксплуатируются на основе неисключительных лицензий, что позволяет большему числу организаций и пользователей использовать программные продукты без необходимости приобретения эксклюзивных прав [3];

2) ИС, использующие модель SaaS: такие системы чаще всего сдают в аренду крупному и малому бизнесу. Модель SaaS предоставляет необходимый функционал заказчикам по подписке, с ограниченным сроком использования;

3) ИС, созданные самостоятельно организациями только для внутреннего пользования;

5) заказные ИС, разрабатываемые внешними организациями по индивидуальным заказам. Такие системы создаются с учетом специальных требований будущего пользователя продукции;

6) бесплатно распространяемые ИС, выпускаемые под лицензиями. Данный тип систем позволяет свободное использование, модификацию и распространение программного обеспечения, что делает их популярными в образовательной и исследовательской среде;

7) ИС учебного характера, которые создаются в основном для демонстрационных или исследовательских целей и не предназначены для длительной эксплуатации. Такие системы широко используются в образовательных учреждениях и для проведения экспериментов в области информационных технологий.

Понимание классификации информационных систем является предварительным этапом для разработки эффективных мер по обеспечению безопасности.

## Методологии анализа угроз и уязвимостей

В связи с постоянным ростом и развитием киберугроз, важной частью для обеспечения безопасности является регулярный анализ угроз и уязвимостей. Рассмотрим и сравним основные популярные методы, используемые для анализа состояния ИС.

*OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)*. Главная суть этой модели заключается в том, что она используется для оценки рисков ИБ только внутри организации, для этого создается специальный отдел, работники которого отвечают за безопасность ИС. В методе OCTAVE процесс работы по оценке рисков проходит в 3 этапа (см. рисунок).

Этап 1. Построение профиля угрозы на основе активов.

Этап 2. Идентификация уязвимостей инфраструктуры.

Этап 3. Разработка стратегии защиты и планов по уменьшению рисков.

Один из самых главных недостатков данного метода заключается в зависимости от квалификации внутренних экспертов организации, при недостаточном количестве знаний оценки рисков могут быть проведены неточно. Также нужно учитывать, что метод OCTAVE дает только качественную оценку [5].

*EBIOS (Expression des Besoins et Identification des Objectifs de Securite)* разработан во Франции агентством ANSSI. Данная методика соответствует современным стандартам кибербезопасности и позволяет адаптировать подходы к управлению рисками в зависимости от целей конкретного проекта [6]. Оценка рисков проходит в 5 этапов.

1. На первом этапе определяют объект исследования и устанавливают базовые требования безопасности.

2. Далее в результате тщательного анализа формируется карта источников риска.

3. На третьем этапе проводится разработка и оценка высокоуровневых сценариев атак, а также выбор мер для обеспечения безопасности ИС. Цель данного этапа – разработка конкретных технических сценариев, по которым злоумышленники могут реализовать атаки. Далее проходит оценка сценариев для определения наиболее критичных направлений атак.

4. На последнем этапе подводятся итоги, определяют меры защиты и устанавливают критерии для дальнейшего мониторинга и анализа рисков.

Для применения метода EBIOS нужно часто проводить встречи и семинары для сбора информации, что выступает в качестве недостатка, так как это влияет на скорость оценки.

В основе метода *STRIDE* лежит работа с 6 типами основных угроз: Spoofing (подмена), Tampering (искажение), Repudiation (отказ от ответственности), Information Disclosure (утечка информации), Denial of Service (отказ в обслуживании) и Elevation of Privilege (повышение привилегий) [1; 4]. Из-за этого одним из главных недостатков STRIDE является ограниченная гибкость.

Каждая из представленных методологий обладает своими плюсами и минусами, и может применяться в зависимости конкретных требований к безопасности информационной системы.

## Анализ угроз в защищенных информационных системах

В независимости от выбора метода общий процесс анализа угроз и уязвимостей проходит в несколько этапов: Идентификация угроз и уязвимостей, оценка рисков, ранжирование угроз.




Этапы метода OCTAVE

Угрозы делятся на два вида:

1) внешние угрозы, исполняемые субъектами, не имеющими доступ к системе, с целью извлечения конфиденциальной информации, нарушения целостности системы или получение контроля над ней;

2) внутренние угрозы представляют собой утечку данных, неправомерное использование привилегий из-за действий сотрудников, умышленно или по неосторожности.

Атаки – это преднамеренные действия злоумышленников, направленные на нарушение, разрушение, получение несанкционированного доступа или изменение информации и ресурсов информационных систем. Основные типы атак:

– вирусы и вредоносное ПО самый распространенный вид угроз, который может не только получать и изменять данные, но и служить начальной точкой для более масштабных атак;

– атаки отказа в обслуживании (DoS и DDoS) направлены на перегрузку системы запросами с целью ее вывода из строя;

– Advanced Persistent Threats (APT) отличаются высокой степенью сложности обнаружения, так как злоумышленники проводят многоступенчатые действия для получения доступа к защищенным фрагментам системы.

Информационные системы сталкиваются с широким спектром угроз, поэтому повышается важность комплексного анализа угроз и совершенствование мер защиты.

## Заключение

Проведенный анализ подтверждает, что в современных условиях информационные системы сталкиваются с широким спектром угроз, как внутри организации, так и внешне, что подчеркивает необходимость комплексного многоуровневого подхода к обеспечению информационной безопасности, включающего как технические, так и организационные меры защиты. Применяемые методологии анализа угроз, такие как OCTAVE, EBIOS и STRIDE, позволяют оценить риски и уязвимости, однако каждая из них имеет свои ограничения, требующие адаптации под специфические условия эксплуатации. В итоге, постоянное обновление и совершенствование систем безопасности, наряду с регулярным анализом угроз и обучением персонала, является залогом надежной защиты данных в условиях развивающегося цифрового пространства.

## *СПИСОК ЛИТЕРАТУРЫ*

1. Дегтярев, Д. И. Безопасная компиляция и архитектуры защищенных модулей / Д. И. Дегтярев, О. А. Какорина // Безопасность информационных систем и технологий в условиях цифровой экономики : материалы IX Всерос. науч.-практ. конф. с междунар. участием (Волгоград, 27–28 окт. 2021 г.). – Волгоград : Волгогр. гос. ун-т, 2021. – С. 23–26.

2. Мелентьева, О. В. Преимущества и недостатки заказных и тиражируемых информационных систем / О. В. Мелентьева // От синергии знаний к синергии бизнеса : сб. ст. и тез. докл. IX Междунар. науч.-практ. конф. студентов, магистрантов и преподавателей (Омск, 8 апр. 2022 г.). – Омск : Издат. центр КАН, 2022.

3. Надежность и качество информационных систем: анализ состава влияющих факторов с позиций информационной безопасности / Ю. М. Брумштейн, О. М. Князева, И. А. Дюдиков, Е. Ю. Васьковский // Надежность и качество : тр. Междунар. симпоз. – 2016. – Т. 1. – С. 101–106.

4. Ноев, А. Н. Моделирование угроз безопасности информации на объектах УИС / А. Н. Ноев, Е. Д. Пономарев // Актуальные проблемы деятельности подразделений УИС : сб. материалов Всерос. науч.-практ. конф. В 2-х т. Т. 1 (Воронеж, 23 окт. 2020 г.). – Воронеж : Воронеж. ин-т Федер. службы исполнения наказаний России, 2020. – С. 187–190.

5. Файзулаев, Д. Ф. Методы и средства анализа рисков информационной безопасности предприятия / Д. Ф. Файзулаев, Б. Б. Морозов // Безопасность информационных технологий. – 2017. – Т. 24, № 3. – С. 69–74.

6. Черняев, М. Д. Методика оценки риска EBIOS / М. Д. Черняев // Управление развитием крупномасштабных систем (MLSD'2023) : тр. шестнадцатой Междунар. конф. (Москва, 26–28 сент. 2023 г.). – М. : Ин-т проблем управления им. В.А. Трапезникова РАН, 2023. – С. 1240–1243. – DOI: 10.25728/mlsd.2023.1240

## *REFERENCES*

1. Degtyarev D.I., Kakorina O.A. Bezopasnaya kompilyaciya i arhitektury zashchishchennyh modulej [Secure Compilation and Architectures of Protected

Modules]. *Bezopasnost informacionnyh sistem i tekhnologij v usloviyah cifrovoj ekonomiki: materialy IX Vseros. nauch.-prakt. konf. s mezhdunar. uchastiem (Volgograd, 27–28 okt. 2021 g.)* [Security of Information Systems and Technologies in the Digital Economy. Proceedings of the 9th All-Russian Scientific and Practical Conference with International Participation. Volgograd, October 27–28, 2021]. Volgograd, Volgogr. gos. un-t, 2021, pp. 23-26.

2. Melentyeva O.V. Preimushchestva i nedostatki zakaznyh i tirazhiruemyh informacionnyh sistem [Advantages and Disadvantages of Custom and Replicated Information Systems]. *Ot sinergii znanij k sinergii biznesa: sb. st. i tez. dokl. IX Mezhdunar. nauch.-prakt. konf. studentov, magistrantov i prepodavatelej (Omsk, 8 apr. 2022 g.)* [From the Synergy of Knowledge to the Synergy of Business. Collection of Articles and Abstracts of Reports of the 9th International Scientific and Practical Conference of Students, Undergraduates and Teachers. Omsk, April 8, 2022]. Omsk, Izdat. centr KAN, 2022.

3. Brumshtein Yu.M., Knyazeva O.M., Dyudikov I.A., Vaskovskij E.Yu. Nadezhnost i kachestvo informacionnyh sistem: analiz sostava vliyayushchih faktorov s pozicij informacionnoj bezopasnosti [Reliability and Quality of Information Systems: Analysis of the Composition of Influencing Factors from the Standpoint of Information Security]. *Nadezhnost i kachestvo: tr. Mezhdunar. simpoz.* [Reliability and Quality. Proceedings of the International Symposium], 2016, vol. 1, pp. 101-106.

4. Noev A.N., Ponomarev E.D. Modelirovanie ugroz bezopasnosti informacii na obyektah UIS [Modeling of Information Security Threats at the Facilities of the Penitentiary System]. *Aktualnye problemy deyatelnosti podrazdelenij UIS: sb. materialov Vseros. nauch.-prakt. konf. V 2-h t. T. 1 (Voronezh, 23 okt. 2020 g.)* [Topical Problems of the Activities of the Penitentiary System Units. Proceedings of the All-Russian Scientific and Practical Conference: In 2 Vols. Vol. 1. Voronezh, October 23, 2020], Voronezh, Voronezh. in-t Feder. sluzhby ispolneniya nakazaniy Rossii, 2020, pp. 187-190.

5. Fajzulaev D.F., Morozov B.B. Metody i sredstva analiza riskov informacionnoj bezopasnosti predpriyatiya [Methods and Means of Information Security Risk Analysis for an Enterprise]. *Bezopasnost informacionnyh tekhnologij* [Information Technology Security], 2017, vol. 24, no. 3, pp. 69-74.

6. Chernyaev M.D. Metodika ocenki riska EBIOS [EBIOS Risk Assessment Methodology]. *Upravlenie razvitiem krupnomasshtabnyh sistem (MLSD'2023): tr. shestnadcatoj Mezhdunar. konf. (Moskva, 26–28 sent. 2023 g.)* [Development of Large-Scale Systems Control (MLSD'2023). Proceedings of the Sixteenth International Conference, Moscow. September 26–28, 2023]. Moscow, In-t problem upravleniya im. V.A. Trapeznikova RAN, 2023, pp. 1240-1243. DOI: 10.25728/mlsd.2023.1240

# ANALYSIS OF THREATS AND VULNERABILITIES IN SECURE INFORMATION SYSTEMS

**Vladislav G. Yarikov**

Candidate of Sciences (Pedagogy),
Associate Professor, Department of Methods for Teaching Mathematics and Physics, ICT,
Volgograd State Social and Pedagogical University
yarikov_vg@mail.ru
Prosp. Lenina, 27, 400005 Volgograd, Russian Federation

**Alexandra N. Panchenko**

Student, Department of Information Security,
Volgograd State University
IBm-241_744165@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

**Abstract.** This article conducts a comprehensive analysis of threats and vulnerabilities within secure information systems, a critical issue exacerbated by the increasing pace of digitalization and the proliferation of sophisticated cyber threats. The study systematically examines the foundational aspects of information security, beginning with a classification of

information systems based on their usage, licensing, and operational models. It further delineates a multi-layered defense strategy encompassing physical, network, application, and organizational levels to ensure robust protection. The core of the analysis focuses on comparing prominent threat assessment methodologies – OCTAVE, EBIOS, and STRIDE – highlighting their unique processes, applications, and inherent limitations for evaluating system risks and vulnerabilities. The research provides a detailed typology of threats, distinguishing between external and internal sources, and analyzes prevalent attack vectors, including viruses/malware, Denial-of-Service (DoS/DDoS) attacks, and complex Advanced Persistent Threats (APTs). The conclusion emphasizes the necessity of a continuous, adaptive, and multi-faceted security approach. It underscores that regular threat analysis, coupled with the ongoing refinement of protective measures and personnel training, is indispensable for maintaining data integrity and confidentiality in the evolving digital landscape.

**Key words:** cybersecurity, threat analysis, vulnerabilities, OCTAVE, EBIOS, STRIDE, DoS/DDoS, Advanced Persistent Threats.