**Автоматизация и моделирование в проектировании и управлении. 2025. № 3 (29). С. 73-79.**
**ISSN 2658-3488 print, ISSN 2658-6436 online**
**Automation and modeling in design and management. 2025. № 3 (29). P. 73-79.**

Научная статья
Статья в открытом доступе
УДК 004.056
doi: 10.30987/2658-6436-2025-3-73-79

# ВЛИЯНИЕ НЕУДОВЛЕТВОРЕННОГО РАБОТНИКА ПРЕДПРИЯТИЯ НА УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Наталия Михайловна Кузнецова[1], Татьяна Владимировна Карлова[2]**
[1] Московский государственный технологический университет «СТАНКИН», г. Москва, Россия
[2] Институт конструкторско-технологической информатики Российской академии наук, г. Москва, Россия
[1] knm87@mail.ru
[2] karlova-t@yandex.ru

**Аннотация.** *Целью научной работы является выявление основных особенностей влияния неудовлетворенного работника предприятия на уровень информационной безопасности. Для достижения поставленной цели, представлены результаты анализа мотивации неудовлетворенного работника. Также предложена методика формирования модели нарушителя – неудовлетворенного работника с помощью базы данных (БД) угроз безопасности информации, сформированной ФСТЭК РФ, а также БД угроз, сформированной MITRE. Новизной работы является предложенная креативная концепция формирования модели нарушителя – неудовлетворенного работника предприятия, основанной на совместном применении БД угроз, сформированных ФСТЭК РФ и MITRE. Результатом исследования являются рекомендации по применению предложенной методики создания модели нарушителя – неудовлетворенного работника предприятия (в том числе работавшего на предприятии ранее).*

**Ключевые слова:** информационная безопасность, защита информации, автоматизация, защита от *APT*, защита от целевых продолжительных атак повышенной сложности

**Для цитирования:** Кузнецова Н.М., Карлова Т.В. Влияние неудовлетворенного работника предприятия на уровень информационной безопасности // Автоматизация и моделирование в проектировании и управлении. 2025. №3 (29). С. 73-79. doi: 10.30987/2658-6436-2025-3-73-79.
Original article
Open Access Article

# THE IMPACT OF AN ENTERPRISE'S DISSATISFIED EMPLOYEE ON THE INFORMATION SECURITY LEVEL

**Natalia M. Kuznetsova[1], Tatiana V. Karlova[2]**
[1] Moscow State University of Technology «STANKIN», Moscow, Russia
[2] Institute for Design-Technological Informatics of the Russian Academy of Sciences, Moscow, Russia
[1] knm87@mail.ru
[2] karlova-t@yandex.ru

**Abstract.** *The aim of this scientific work is to identify the main features of the impact of an enterprise's dissatisfied employee on the information security level. To achieve this aim, the work presents the results of a dissatisfied employee's motivation analysis; proposes a methodology for forming a model of a violator-a dissatisfied employee using a database (DB) of information security threats formed by the Federal Service for Technical and Export Control (FSTEC) of Russia, as well as a DB of threats formed by MITRE. The novelty of the work lies in the proposed creative concept of forming a model of a violator-an enterprise's dissatisfied employee, based on the joint application of DBs of threats formed by FSTEC and MITRE. The result of the study are recommendations for applying the proposed methodology for creating a model of a violator-an enterprise's dissatisfied employee (including those who previously worked at the enterprise).*

**Keywords:** information security, information protection, automation, protection from *APT*, protection against targeted prolonged attacks of increased complexity

**For citation:** Kuznetsova N.M., Karlova T.V. The Impact of an Enterprise's Dissatisfied Employee on the Information Security Level. Automation and modeling in design and management, 2025, no. 3 (29). pp. 73-79. doi: 10.30987/2658-6436-2025-3-73-79.

## Введение

Для современных транспортных и промышленных предприятий, относящихся к объектам критической информационной инфраструктуры (КИИ), решение задачи обеспечения информационной безопасности является актуальной проблемой. В свою очередь, неудовлетворенный работник предприятия может стать источником угроз, а также повлиять на уровень информационной безопасности. Целью работы является исследование степени влияния неудовлетворенного работника транспортного предприятия на уровень информационной безопасности.

На данный момент наиболее опасными считаются атаки класса *Advanced Persistent Threats* – целевые продолжительные атаки повышенной сложности (*APT*) [1 – 8].

При этом одной из особенностей данных атак является использование трудовых ресурсов предприятия в качестве механизма преодоления систем защиты. При реализации *APT* злоумышленники применяют методы социальной инженерии. Неудовлетворенный работник становится объектом угрозы.

Кроме того, неудовлетворенный работник предприятия может по собственной воле оказаться субъектом угрозы.

## Мотивация неудовлетворенного работника предприятия

Согласно принятой модели мотивации работников предприятия, основными факторами являются: внешний (размер материальных вознаграждений работников); внутренний (психологический аспект); социальный (льготы, пособия, дополнительные стимулирующие выплаты и т.д.) [9, 10].

Если социальный фактор мотивации регулируется нормами и законами на государственном уровне, то управление внешним и внутренним факторами мотивации работников напрямую зависит от рациональности принятых решений руководством предприятия.

Согласно рис. 1, на удовлетворенность своей работой сотрудника предприятия в первую очередь влияют внешний и внутренний факторы мотивации.

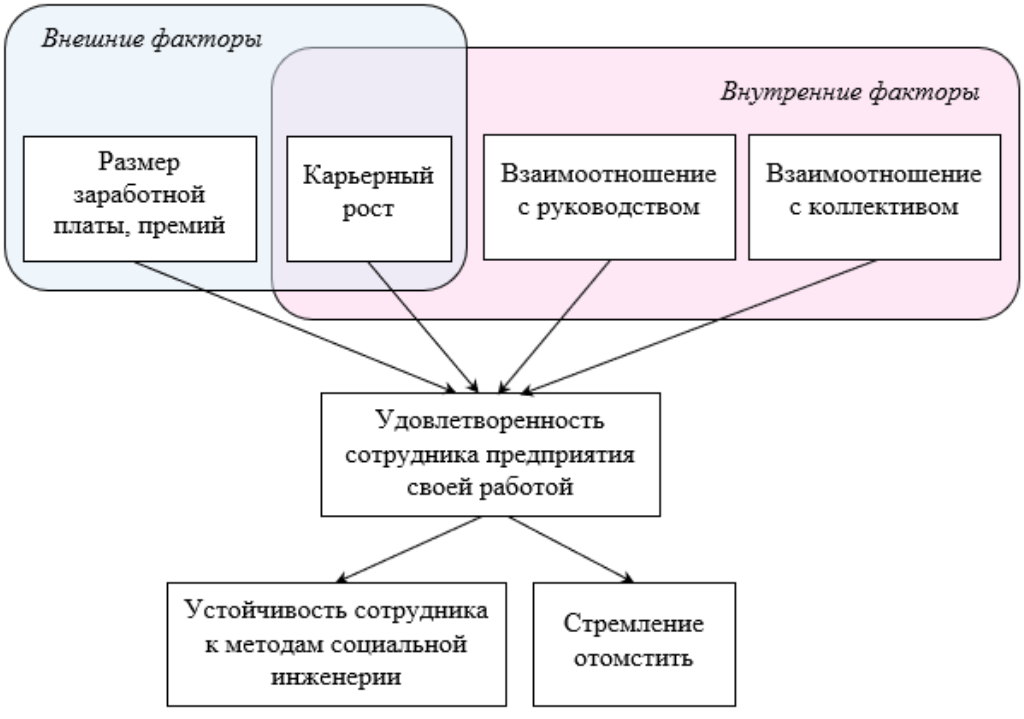


**Рис. 1. Влияние фактором мотивации на неудовлетворенность работника**
***Fig. 1. The influence of motivation factors on employee dissatisfaction***

Важно отметить, что «карьерный рост» относится как к внешнему, так и к внутреннему факторам мотивации работников предприятия.

Удовлетворенность сотрудника предприятия своей работой напрямую влияет на его устойчивость к методам социальной инженерии и на стремление отомстить.

Для полной оценки устойчивости сотрудника к методам социальной инженерии и стремления отомстить необходимо помимо факторов внешней и внутренней мотивации учитывать психологическое состояние работника. В данном исследовании представлен пример оценки удовлетворенности в зависимости от внешних и внутренних факторов мотивации.

В табл. 1 представлен пример назначения весов факторов мотивации по 10-ти балльной шкале.

Значение каждого фактора мотивации определяется экспертной группой эмпирическим путем.

Таблица 1

**Пример назначения весов факторам мотивации**

*Table 1*

***Example of assigning weights to motivation factors***

| | Фактор мотивации | Вес ($w$) |
|---|---|---|
| 1 | Размер заработной платы | 8 |
| 2 | Карьерный рост | 10 |
| 3 | Взаимоотношением с руководством | 7 |
| 4 | Взаимоотношение с коллективом | 6 |

## Формирование модели нарушителя с помощью БД угроз безопасности информации ФСТЭК РФ

Согласно БД угроз безопасности информации АСУ ТП, сформированной ФСТЭК РФ [11], в качестве источника угроз (характеристики и потенциала нарушителя) – субъекта угрозы – выступают:

– внешний нарушитель с высоким потенциалом;

– внешний нарушитель со средним потенциалом;

– внешний нарушитель с низким потенциалом;

– внутренний нарушитель с высоким потенциалом;

– внутренний нарушитель со средним потенциалом;

– внутренний нарушитель с низким потенциалом.

Категория «неудовлетворенный работник предприятия» может относиться к любому источнику угроз:

– внутренний нарушитель (со средним, низким потенциалом) – сотрудник предприятия;

– внутренний нарушитель (с высоким потенциалом) – сотрудник отдела информационной безопасности предприятия;

– внешний нарушитель (со средним, низким потенциалом) – сотрудник, ранее работавший на предприятии;

– внешний нарушитель (с высоким потенциалом) – сотрудник, ранее работавший на предприятии в отделе информационной безопасности.

База данных угроз безопасности информации ФСТЭК РФ сформирована таким образом, что для отдельного вида ресурса (объекта угроз) ставится в соответствие возможные сценарии реализации и субъекты угроз.

## Формирование модели нарушителя с помощью БД *MITRE*

Концепция формирования модели угроз *MITRE* состоит в составлении списка тактик и техник угроз относительно этапа реализации угрозы.

Для каждой тактики в БД *MITRE* сформирован список техник.

Всего в БД *MITRE* 14 тактик:

– «*Reconnaissanse*» (этап разведки) – включает 10 техник;

– «*Resource Development*» (этап исследования и анализа структуры ресурсов – объекта угрозы) – включает 8 техник;

– «*Initial Access*» (первоначальный, первичный доступ) – включает 10 техник;
– «*Execution*» (этап исполнения) – включает 14 техник;
– «*Presistence*» (этап закрепления) – включает 20 техник;
– «*Privilege Escalation*» (этап увеличения прав и привилегий) – включает 14 техник;
– «*Defense Evasion*» (этап «уклонения» от механизмов защиты) – включает 44 техник;
– «*Credential Access*» (получение доступа к учетным данным) – включает 17 техник;
– «*Discovery*» (этап детального и полного анализа) – включает 32 техники;
– «*Lateral Movement*» (этап расширения объема проникновения) – включает 9 техник;
– «*Collection*» (этап сбора) – включает 17 техник;
– «*Command and Control*» (этап захвата управления) – включает 18 техник;
– «*Exfiltration*» (этап извлечения ресурсов) – включает 9 техник;
– «*Impact*» (этап воздействия на ресурсы) – включает 14 техник [1, 12].

При этом фокус внимания *MITRE* направлен на поведение субъекта угрозы (злоумышленника).

База данных *MITRE* сформирована таким образом, что для отдельного этапа реализации угрозы злоумышленником (субъектом угрозы) ставится в соответствие возможные атакуемые ресурсы предприятия (объекты угрозы).

## Методика создания модели нарушителя – неудовлетворенного работника предприятия на основе БД угроз безопасности информации, сформированной ФСТЭК РФ, и БД угроз, сформированной *MITRE*

На рис. 2 представлена схема создания модели нарушителя – неудовлетворенного работника предприятия на основе БД угроз, сформированной ФСТЭК РФ, и БД угроз, сформированной *MITRE* [1, 11, 12].


**Рис. 2. Схема формирования модели нарушителя – неудовлетворенного работника предприятия на основе БД угроз, сформированной ФСТЭК РФ, и БД угроз, сформированной *MITRE***
***Fig. 2. Scheme for forming a model of an intruder – a dissatisfied employee of an enterprise based on a threat database generated by the FSTEC of the Russian Federation and a threat database generated by MITRE***

Согласно рис. 2, работа с БД угроз ФСТЭК РФ предполагает направление анализа от объекта угрозы (ресурсу предприятия) к субъекту угрозы (человеку), в то время как работа с БД угроз *MITRE* предполагает противоположное направление анализа – от субъекта к объекту угрозы.

Для модели нарушителя – неудовлетворенного работника предприятия разумно предположить следующие характеристики субъекта угрозы: уровень мотивации к мести; уровень моральной устойчивости; уровень квалификации; степень осведомленности об объекте угрозы (параметрах ресурсов предприятия); степень осведомленности о субъекте защиты (об используемых методах защиты).

В табл. 2 представлен пример соответствия характеристик субъекта угрозы, модели нарушителя и степени серьёзности потенциальной угрозы.

Степень серьезности потенциальной угрозы определяется экспертным методом по шкале от 1 до 10, при этом 1 – самая низкая серьёзность угрозы, 10 – самая высокая серьезность угрозы.

Таблица 2

**Соответствие характеристик субъекта угрозы и модели нарушителя степени серьёзности потенциальной угрозы**

*Table 2*

***Correspondence between the characteristics of the threat subject and the intruder model to the degree of seriousness of the potential threat***

| | | Категория нарушителя | | | |
|---|---|---|---|---|---|
| | | Нарушитель – сотрудник предприятия | Нарушитель – сотрудник отдела информационной безопасности предприятия | Нарушитель – сотрудник, ранее работавший на предприятии | Нарушитель – сотрудник, ранее работавший в отделе информационной безопасности предприятия |
| Характеристики нарушителя | Высокий уровень мотивации к мести | 8 | 10 | 7 | 8 |
| | Низкий уровень мотивации к мести | 1 | 1 | 1 | 1 |
| | Низкий уровень моральной устойчивости | 7 | 10 | 6 | 10 |
| | Высокий уровень моральной устойчивости | 1 | 1 | 1 | 1 |
| | Высокий уровень квалификации | 9 | 10 | 8 | 9 |
| | Низкий уровень квалификации | 2 | 3 | 1 | 1 |
| | Высокая степень осведомленности об объекте угрозы | 9 | 10 | 8 | 9 |
| | Низкая степень осведомленности об объекте угрозы | 2 | 2 | 1 | 2 |
| | Высокая степень осведомленности о субъекте защиты | 9 | 10 | 8 | 10 |
| | Низкая степень осведомленности о субъекте защиты | 3 | 3 | 2 | 3 |
| Интегральный показатель по категории нарушителя | | 51 | 60 | 43 | 54 |

Таким образом, самая высокая серьезность потенциальной угрозы соответствует нарушителю:

– сотрудник отдела информационной безопасности с:

а) высоким уровнем мотивации к мести;

б) низким уровнем моральной устойчивости;

в) высоким уровнем квалификации;

г) высокой степенью осведомленности об объекте угрозы;

д) высокой степенью осведомленности о субъекте защиты;

– сотрудник, ранее работавший в отделе информационной безопасности с:

а) низким уровнем моральной устойчивости;

б) высокой степенью осведомленности о субъекте защиты.

В свою очередь, наименьшую опасность представляют (низкую степень потенциальной угрозы) представляют сотрудники:

– с низким уровнем мотивации;
– высоким уровнем моральной устойчивости;
– низкой степенью осведомленности об объекте угрозы и о субъекте защиты.

Наивысший интегральный показатель по категории нарушителя – сотрудника предприятия у категории «сотрудник отдела информационной безопасности предприятия», наименьший – сотрудника предприятия у категории «сотрудник, ранее работавший на предприятии».

## Заключение

Таким образом, проведенный анализ показал, что наиболее опасным является нарушитель категории «сотрудник отдела информационной безопасности предприятия» ввиду того, что именно он обладает высоким уровнем квалификации, высокой степенью осведомленности об объекте угрозы и о субъекте защиты.

При оценке общего уровня информационной безопасности предприятия необходимо формировать модель нарушителя-злоумышленника, включающую работника предприятия, в том числе ранее работавшего, в том числе в отделе информационной безопасности предприятия.

Для формирования модели нарушителя целесообразно совместное применение двух БД угроз, сформированных ФСТЭК РФ [11] и *MITRE* [12]. Таким образом производится анализ сценариев реализации угрозы сразу в двух направлениях: от объекта к субъекту угрозы (на основе БД угроз безопасности информации, сформированной ФСТЭК РФ), а также от субъекта к объекту (на основе БД угроз, сформированной *MITRE*). Данный подход обеспечит комплексность, высокую надежность и точность анализа информации и дальнейшего моделирования поведения злоумышленника.

Кроме того, представленная в статье методика формирования модели нарушителя позволит повысить уровень информационной безопасности ресурсов транспортного предприятия за счет своевременного выявления недобросовестных работников.

### Список источников:


1. Кузнецова Н.М. Методология защиты от целевых кибератак повышенной сложности в автоматизированных системах промышленного предприятия (монография). – М.: «Янус-К», 2024. – 132 с.
2. Кузнецова Н.М., Карлова Т.В. , Бекмешов А.Ю. Решение задачи автоматизации процессов защиты стратегически важных ресурсов предприятия от комплексных кибер-атак на основе анализа тактик злоумышленников // Вестник Брянского государственного технического университета. – 2020. – № 7(92). – С. 48-53.
3. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Yu. Method of Timely Prevention from Advanced Persistent Threats on the Enterprise Automated Systems // 2022 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)
4. Karlova T.V., Kuznetsova N.M., Sheptunov S.A., Bekmeshov A.Yu. Methods Dedicated to Fight Against Complex Information Security Theats on Automated Factories Systems // 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS) // Proceedings. – М.: Фонд «Качество». – 2016. – P. 23-27.
5. Кузнецова Н.М., Карлова Т.В., Бекмешов А.Ю. Построение модульной структуры автоматизированной системы комплексного обеспечения защиты стратегически важных ресурсов предприятия транспорта / Н.М. Кузнецова // Вестник Брянского государственного технического университета. 2021. – № 9 (106). – С. 36-42.


### References:


1. Kuznetsova N.M. Methodology of Protection Against Targeted Cyber Attacks of Increased Complexity in Automated Systems of an Industrial Enterprise. Moscow: Janus-K; 2024.
2. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Yu. Solution of Protection Automation Problem of Company Strategic Resources Against Complex Cyberattacks Based on Criminal Tactics Analysis. Bulletin of Bryansk State Technical University. 2020;7(92):48-53.
3. Kuznetsova NM, Karlova TV, Bekmeshov AYu. Method of Timely Prevention from Advanced Persistent Threats on the Enterprise Automated Systems. In: Proceedings of the 2022 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS); Saint Petersburg: 2022. p. 158-161.
4. Karlova TV, Kuznetsova NM, Sheptunov SA, Bekmeshov AYu. Methods Dedicated to Fight Against Complex Information Security Threats on Automated Factories Systems. In: Proceedings of the 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS). Moscow: Quality Fund: 2016. p. 23-27.
5. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Yu. Construction of a Modular Structure of an Automated System for Integrating Support for the Protection of Strategically Important Resources of a Transport Enterprise. Bulletin of Bryansk State Technical University. 2021;9(106):36-42.

6. Кузнецова Н.М., Карлова Т.В. Основные принципы защиты автоматизированных систем крупных промышленных предприятий от комплексных кибер-атак // Вестник Брянского государственного технического университета. – 2017. – № 4 (57). – С. 84-89.

7. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Yu. Protection the Data Banks in State Critical Information Infrastructure Organizations // Proceedings of the 2019 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies» (IT&QM&IS), Sochi, Russia, 23-27 September 2019. – P.155–157.

8. Кузнецова Н.М., Карлова Т.В., Бекмешов А.Ю. Анализ кибер-угроз, направленных на программно-аппаратное обеспечение робототехнических и автоматизированных систем масштаба предприятия, и способы их предотвращения // Качество. Инновации. Образование. – 2016. – № S2 (129). – С. 165-170.

9. Ефимов В.В. Средства и методы управления качеством: учебное пособие. – М.: КНОРУС, 2007. – 232 с.

10. Кузнецова Н.М., Карлова Т.В. Всеобщее управление качеством. Решение задачи повышения уровня информационной безопасности в рамках комплексного обеспечения качества на промышленном предприятии (Курс лекций, лабораторный практикум). Учебное пособие. – М.: Янус-К, 2019. – 64 с.

11. БДУ – Угрозы – ФСТЭК России [Электронный ресурс] / режим доступа URL: https://bdu.fstec.ru (дата обращения: 12.02.2025)

12. MITRE ATT&CK [Электронный ресурс] / режим доступа URL: https://attackmitre.org (дата обращения: 12.02.2025)

6. Kuznetsova N.M., Karlova T.V. Basic Principles for Large Enterprise Automated System Protection Against Cyber Attacks. Bulletin of Bryansk State Technical University. 2017;4(57):84-89.

7. Kuznetsova NM, Karlova TV, Bekmeshov AYu. Protection the Data Banks in State Critical Information Infrastructure Organizations. In: Proceedings of the 2019 IEEE International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS); 2019 Sep 23-27; Sochi, Russia: 155-157.

8. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Yu. Analysis of Cyber-Threats Directioned to Software and Hardware of Robotic and Automated Control Systems and Methods of Defense. Quality. Innovations. Education. 2016;S2(129):165-170.

9. Efimov V.V. Means and Methods of Quality Management. Moscow: Knorus; 2007.

10. Kuznetsova N.M., Karlova T.V. Total Quality Management. Solving the Problem of Increasing the Level of Information Security at an Industrial Enterprise as Part of Quality Management System. Moscow: Janus K; 2019.

11. Databank of Security Threats – Threats – Federal Service for Technical and Export Control of Russia [Internet] [cited 2025 Feb 12]. Available from: https://bdu.fstec.ru

12. MITRE ATT&CK [Internet] [cited 2025 Feb 12]. Available from: https://attackmitre.org

**Информация об авторах:**

**Кузнецова Наталия Михайловна**
кандидат технических наук, доцент Московского государственного технологического университета «СТАНКИН»

**Карлова Татьяна Владимировна**
доктор социологических наук, кандидат технических наук, профессор Института конструкторско-технологической информатики Российской академии наук

**Information about the authors:**

**Kuznetsova Natalia Mikhailovn**a
Candidate of Technical Sciences, Associate Professor of Moscow State University of Technology «STANKIN»

**Karlova Tatyana Vladimirovna**
Doctor of Sociological Sciences, Candidate of Technical Sciences, Professor of the Institute for Design-Technological Informatics of the Russian Academy of Sciences

**Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.**
**Contribution of the authors: the authors contributed equally to this article.**

**Авторы заявляют об отсутствии конфликта интересов.**
**The authors declare no conflicts of interests.**

**Статья поступила в редакцию 13.03.2025; одобрена после рецензирования 03.04.2025; принята к публикации 23.04.2025.**

**The article was submitted 13.03.2025; approved after reviewing 03.04.2025; accepted for publication 23.04.2025.**

**Рецензент –** Пугачев А.А., доктор технических наук, доцент, Брянский государственный технический университет.

**Reviewer –** Pugachev A.A., Doctor of Technical Sciences, Associate Professor, Bryansk State Technical University.