УДК 004.056
DOI 10.33764/2618-981X-2023-6-165-170

Е. Б. Маркелова[1], А. В. Троеглазова[1]*

Оценка факторов, оказывающих влияние на реализацию угроз информационной безопасности

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: Markelova-EB2021@sgugit.ru

Аннотация. Важнейшим этапом разработки и совершенствования защищенной системы электронного документооборота является выявление угроз информационной безопасности, а также факторов, оказывающих влияние на их реализацию. Математическая оценка значимости влияния этих факторов необходима для построения эффективной системы защиты информации, обрабатываемой в системе электронного документооборота. Целью данной работы является математическая оценка факторов, оказывающих влияние на реализацию угроз безопасности информации, обрабатываемой в системе электронного документооборота, методом дробного факторного планирования эксперимента. Оценка рисков была произведена для группы угроз, реализуемых в государственной организации внутренним нарушителем с низким потенциалом, и изучено влияние факторов несанкционированного доступа к аутентификационной информации, устаревших антивирусных баз и отсутствия запрета на запуск исполняемых файлов от имени пользователей. Рассмотренный подход может быть применим и к автоматизированной системе, и к системам обработки информации без использования средств автоматизации.

Ключевые слова: угрозы информационной безопасности, система электронного документооборота, оценка вероятности, факторное планирование эксперимента

E. B. Markelova[1], A. V. Troeglazova[1]*

Assessment of Factors Influencing the Implementation of Information Security Threats

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: Markelova-EB2021@sgugit.ru

Abstract. The most important stage in the development and improvement of a secure electronic document management system is the identification of threats to information security, as well as factors that affect their implementation. A mathematical assessment of the significance of the influence of these factors is necessary to build an effective system for protecting information processed in an electronic document management system. The purpose of this work is a mathematical assessment of the factors influencing the implementation of threats to the security of information processed in the electronic document management system using the method of fractional factorial planning of the experiment. The risk assessment was carried out for a group of threats implemented in a government organization by an insider with low potential and the impact of factors of unauthorized access to authentication information, outdated anti-virus databases and the absence of a ban on running executable files on behalf of users was studied. The considered approach can be applied both to an automated system and to information processing systems without the use of automation tools.

Keywords: information security threats, electronic document management system, probability assessment, factorial planning of experiment

Введение

Для создания в организации защищенного электронного документооборота необходимо обеспечить аутентификацию пользователей и разделение прав доступа к электронным документам, подтвердить авторство документов в системе электронного документооборота, реализовать важнейшие свойства информации (конфиденциальность, целостность, доступность) за счет обеспечения юридической значимости электронных документов [1]. Наиболее распространенными угрозами, реализуемыми при эксплуатации систем электронного документооборота, являются угроза неправомерного ознакомления с информацией, угроза несанкционированного копирования информации, угроза внедрения кода или данных, угроза распространения «почтовых червей», угроза заражения компьютера при посещении неблагонадежных сайтов, угроза несанкционированной модификации защищаемой информации, «кража» учетной записи доступа к сетевым сервисам, угроза приведения системы в состояние «отказ в обслуживании» (DOS), угроза утраты носителей информации [2, 3].

Важнейшим этапом разработки и совершенствования системы защиты информации, обрабатываемой в системе электронного документооборота, является выявление и количественная оценка факторов, оказывающих влияние на реализацию угроз информационной безопасности. В литературе описаны различные методы – как качественные, так и количественные [4-6], широкое распространение среди которых получил метод факторного планирования эксперимента [5-8].

Цель настоящей работы заключается в математической оценке факторов, оказывающих влияние на реализацию угрозы безопасности информации, обрабатываемой в СЭД, методом дробного факторного планирования эксперимента.

Методы и материалы

Модель угроз безопасности информации, обрабатываемой в системе электронного документооборота, составлена в соответствии с требованиями Методического документа «Методика оценки угроз безопасности информации» (утв. ФСТЭК от 5 февраля 2021 г.) [9] и на основании банка угроз [10]. Оценку рисков выполняли для группы угроз, реализуемых в государственной организации внутренним нарушителем с низким потенциалом, что приводит к нарушению конфиденциальности, целостности и доступности информации [10]:

– УБИ.074 – угроза несанкционированного доступа к аутентификационной информации;

– УБИ.086 – угроза несанкционированного изменения аутентификационной информации;

– УБИ.088 – угроза несанкционированного копирования защищаемой информации;

– УБИ.152 – угроза удаления аутентификационной информации;

– УБИ.167 – угроза заражения компьютера при посещении неблагонадёжных сайтов;

– УБИ.168 – угроза «кражи» учётной записи доступа к сетевым сервисам;

– УБИ.172 – угроза распространения «почтовых червей»;

– УБИ.191 – угроза внедрения вредоносного кода в дистрибутив программного обеспечения.

Процесс оценки вероятности реализации угроз методом дробного факторного планирования эксперимента представлен на рис. 1 [5, 6].

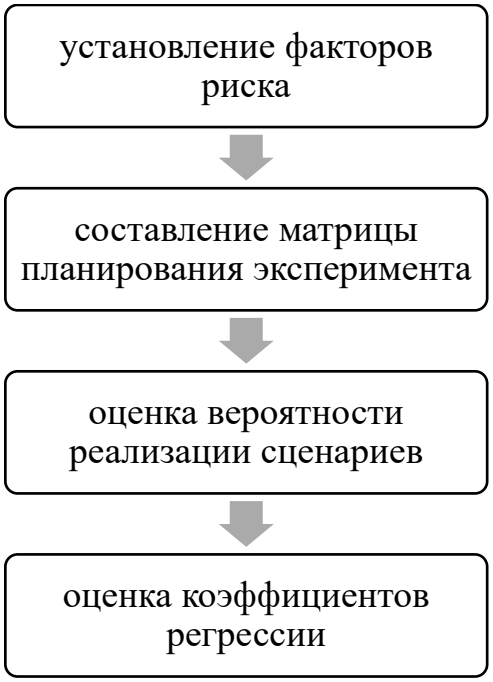

Рис. 1. Процесс оценки вероятности реализации угроз методом дробного факторного планирования эксперимента

Математическая модель реализации угрозы информационной безопасности для дробного факторного эксперимента может быть представлена в виде линейной регрессионной зависимости:

$$Y = b_0 + \sum_{i=1}^{k} b_i X_i + \sum_{i,j=1}^{k} b_{ij} X_i X_j + \ldots + \sum_{i,j,n=1}^{k} b_{ijn} X_i X_j X_n , \quad (1)$$

где Y – вероятность реализации угрозы; X_i – значения факторов; b_0 – свободный член; b_i – коэффициент линейного воздействия факторов; b_{ij} – коэффициент взаимодействия факторов; b_{ijn} – коэффициент n-го взаимодействия факторов; i, j, n – номер фактора.

Факторы X_i могут принимать только одно из двух значений: минус 1 – если рассматриваемый фактор не оказывает влияния на реализацию угрозы; плюс 1 – если реализация угрозы зависит от наличия или отсутствия рассматриваемого фактора. Коэффициенты регрессии определяются по формуле:

$$b_j = \frac{\sum_{i-1}^{N} X_{ij} Y_i}{N}. \quad (2)$$

Количество реализуемых сценариев (экспериментов) в факторном дробном эксперименте определяется по следующей формуле:

$$N = 2^{k-p}, \quad (3)$$

где N – количество сценариев (экспериментов); k – количество рассматриваемых факторов; p – целое положительное количество факторов, выведенных путем замены незначимых взаимодействий.

Значения вектор-столбца X_0 во всех сценариях приняты равными +1, поэтому p=1. При условии рассмотрения влияния четырех факторов на реализацию угроз информационной безопасности количество сценариев (экспериментов) составляет 8.

Вероятность реализации угроз для каждого сценария (Y_{ij}) оценивается экспертным методом (метод непосредственного оценивания) по шкале от 0,00 до 1,00. Метод предполагает присваивание объектам экспертизы (каждому сценарию) баллов каждым экспертом, при этом наиболее значимому объекту (сценарию) присваивается наибольшее количество баллов согласно установленной шкале. Вероятность реализации угроз для каждого сценария (Y_i) оценивается как среднее арифметическое значение оценок сценариев каждым из четырех экспертов.

Результаты

В качестве причин реализации угрозы несанкционированного доступа к аутентификационной информации (УБИ.074 [10]) можно назвать следующие:

1) небрежность персонала в информационном измерении;

2) устаревшие антивирусные базы;

3) отсутствие запрета на запуск исполняемых файлов от имени пользователей;

4) возможность управления функционированием антивирусного программного обеспечения от имени пользователей.

Матрица планирования эксперимента, составленная для восьми сценариев реализации угроз информационной безопасности, представлена в табл. 1.

Результаты оценки вероятности реализации угроз информационной безопасности экспертным методом представлены в табл. 2.

На основании результатов оценки вероятностей реализации угрозы (табл. 2) для восьми сценариев, представленных в табл. 1, была произведена оценка коэффициентов регрессии по формуле (2). Для четырехфакторного планирования эксперимента уравнение регрессии:

$$Y = 0,669 + 0,064X_1 + 0,076X_2 + 0,171X_3 + 0,019X_4 + 0,001X_1X_2 - 0,019X_1X_3 + 0,009X_2X_3 . \quad (4)$$

Таблица 1

Матрица планирования эксперимента

N	X_0	X_1	X_2	X_3	X_4	X_1X_2	X_1X_3	X_2X_3	Y_i
1	+	–	–	–	–	+	+	+	Y_1
2	+	+	–	–	+	–	–	+	Y_2
3	+	–	+	–	+	–	+	–	Y_3
4	+	+	+	–	–	+	–	–	Y_4
5	+	–	–	+	+	+	–	–	Y_5
6	+	+	–	+	–	–	+	–	Y_6
7	+	–	+	+	–	–	–	+	Y_7
8	+	+	+	+	+	+	+	+	Y_8

Таблица 2

Результаты оценки вероятности реализации угроз
методом непосредственного оценивания

N	Ранги, присвоенные экспертами R_{ij}				$\sum_{i=1}^{n} R_{ij}$	Y_i
	1	2	3	4		
1	0,30	0,30	0,30	0,40	1,30	0,33
2	0,50	0,50	0,50	0,60	2,10	0,53
3	0,40	0,60	0,50	0,50	2,00	0,50
4	0,50	0,70	0,60	0,70	2,50	0,63
5	0,80	0,70	0,80	0,60	2,90	0,73
6	0,70	0,80	0,80	0,80	3,10	0,78
7	0,85	1,00	0,90	0,70	3,45	0,86
8	1,00	1,00	0,95	1,00	3,95	0,99

Каждый коэффициент регрессии играет определенную роль в установлении актуальности угрозы несанкционированного доступа к аутентификационной информации. Так, превышение свободным членом b_0 значения 0,50 свидетельствует об актуальности рассматриваемой угрозы и значимости влияния каждого из четырех рассмотренных факторов на реализацию угрозы информационной безопасности. Третий фактор, отсутствие запрета на запуск исполняемых файлов от имени пользователей, вносит наибольший вклад в реализацию угрозы информационной безопасности и усиливает негативное действие второго фактора (устаревших антивирусных баз) и ослабляет действие первого фактора (небрежность персонала в информационном измерении). Наименьшее влияние на реализацию угрозы оказывает четвертый фактор – возможность управления функцио-

нированием антивирусного программного обеспечения от имени пользователей. Результаты оценки коэффициентов регрессии позволяют осуществлять непрерывный мониторинг выявленных факторов риска.

Заключение

Таким образом, методом дробного факторного эксперимента проведена математическая оценка факторов, оказывающих влияние на угрозу несанкционированного доступа к аутентификационной информации. Было изучено влияние следующих факторов: небрежность персонала в информационном измерении, устаревшие антивирусные базы, отсутствие запрета на запуск исполняемых файлов от имени пользователей, возможность управления функционированием антивирусного программного обеспечения от имени пользователей. Применение рассмотренного подхода позволяет оценить вероятные риски на основе анализа результатов экспертной оценки вероятности реализации угрозы для восьми сценариев.

Методика может быть одинаково применима и к автоматизированной информационной системе, и к системам обработки информации без использования средств автоматизации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Булдакова Т.И., Глазунова Б.В., Ляпина Н.С. Оценка эффективности защиты систем электронного документооборота // Доклады ТУСУРа. – 2012. – № 1 (25), часть 2. – С. 52-56.
2. Заводцев И.В., Борисов М.А., Бондаренко Н.Н., Мелешко В.А. Моделирование угроз безопасности информации и определение их актуальности для информационных систем объектов информатизации федеральных органов исполнительной власти // Computational nanotechnology. – 2022. – № 1, Т. 9. – С. 106-114.
3. Майстренко В.А., Безродных О.А., Дорохин Р.А. Методика определения актуальных угроз безопасности информации в медицинской информационной системе // Омский научный вестник. – 2021. – № 5 (179). – С. 74-79.
4. Миков Д.А. Анализ методов и средств, используемых на различных этапах оценки рисков информационной безопасности // Вопросы кибербезопасности. – 2014. – № 4 (7). – С. 49-54.
5. Белов В.М., Белкин С.А. Оценка вероятности угрозы заражения компьютерным вирусом на основе факторного планирования эксперимента // Информационное противодействие угрозам терроризма. – 2014. – № 23. – С. 55–61.
6. Плетнев П.В., Белов В.М., Зубков Е.В., Крыжановская О.А. К вопросу об определении угроз и рисков информационной безопасности с использованием сценарного подхода и факторного планирования эксперимента // Вестник СибГУТИ. – 2016. – № 4. – С. 12-18.
7. Ильченко Л.М., Брагина Е.К., Егоров И.Э., Зайцев С.И. Расчет рисков информационной безопасности телекоммуникационного предприятия // Открытое образование. – 2018. – Т. 22. – № 2. – С. 62-70.
8. Котенко Д.А. Метод оценки риска информационной безопасности на основе сценарного логико-вероятностного моделирования. – автореферат дисс. на соиск. ученой степени канд.технич.наук. – СПб, 2010. – 18 с.
9. Методический документ «Методика оценки угроз безопасности информации» (утв. ФСТЭК 05.02.2021 г.).
10. Банк данных угроз безопасности информации [сайт]. URL: https://bdu.fstec.ru/threat.