Научная статья
УДК 002.5:004
DOI: 10.14529/ctcr240103

ПОДХОДЫ К ОЦЕНКЕ ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ С КРИПТОГРАФИЧЕСКИМ ПРЕОБРАЗОВАНИЕМ ОБЪЕКТОВ

***Л.А. Артюшина**, larisa-artusina@yandex.ru, https://orcid.org/0000-0001-5160-5294*
***Д.А. Полянский**, polyansk@rambler.ru*
Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Владимир, Россия

Аннотация. Файловая система является одним из компонентов информационной системы, особенно уязвимых к атакам злоумышленников. Следовательно, повышение уровня защищённости информационной системы невозможно без обеспечения достаточного уровня защиты объектов файловой системы, атаки на которые затрагивают в том числе интересы пользователей информационных систем. Для принятия решений по использованию тех или иных механизмов защиты объектов файловой системы необходима регулярная оценка их текущего уровня защищённости. **Цель исследования:** построение модели оценки защищённости информационной системы с криптографическим преобразованием объектов файловой системы в условиях применения злоумышленником широкого спектра атак на файловую систему. **Материалы и методы.** Анализ научных публикаций по проблеме оценки защищённости информационных систем позволил предложить методику оценки защищённости активов информационной системы. Методика основывается на комбинации вероятностного подхода к анализу возможных сценариев реализации угроз в информационных системах для объектов файловой системы, экспертных оценок базовых событий атаки и представления в виде деревьев атак. Представление реализации угроз в виде деревьев атак использовано для моделирования действий злоумышленника. **Результаты.** Разработана структурная модель информационной системы с криптографическим преобразованием объектов. Выделены её ценные активы. Определён перечень основных угроз информационной безопасности, актуальных для такого рода систем. Смоделированы возможные варианты путей реализации атак и возможные сценарии развития событий в процессах передачи объектов файловой системы с криптографическим преобразованием. Предложен комплекс мер защиты объектов информационной системы с криптографическим преобразованием объектов. Предложен расчёт вероятностей атак на актив по пути, определённому деревом атак, возможности реализации атаки, степени эффективности предлагаемых контрмер. **Заключение.** Представленная методика оценки защищённости информационной системы с криптографическим преобразованием объектов даёт возможность комплексного применения известных подходов, будет полезна разработчикам и исследователям в практической и научной деятельности по обеспечению информационной безопасности.

Ключевые слова: информационная безопасность, оценка защищённости, вероятностный подход, деревья атак

Для цитирования: Артюшина Л.А., Полянский Д.А. Подходы к оценке защищённости информационных систем с криптографическим преобразованием объектов // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». 2024. Т. 24, № 1. С. 32–43. DOI: 10.14529/ctcr240103

Original article
DOI: 10.14529/ctcr240103

APPROACHES TO ASSESSING THE SECURITY OF INFORMATION SYSTEMS WITH CRYPTOGRAPHIC TRANSFORMATION OF OBJECTS

***L.A. Artyushina**, larisa-artusina@yandex.ru, https://orcid.org/0000-0001-5160-5294*
***D.A. Polyansky**, polyansk@rambler.ru*
Vladimir State University named after Alexander and Nicolay Stoletovs, Vladimir, Russia

Abstract. The file system is one of the components of an information system, especially vulnerable to attacks by intruders. Consequently, it is impossible to increase the security level of an information system without ensuring a sufficient level of protection for file system objects, attacks on which affect, among other things, the interests of users of information systems. In order to make decisions on the use of certain mechanisms for protecting file system objects, a regular assessment of their current level of security is necessary. **The purpose of the study.** Building a model for assessing the security of an information system with cryptographic transformation of file system objects in the context of an attacker using a wide range of attacks on the file system. **Materials and methods.** The analysis of scientific publications on the problem of assessing the security of information systems allowed us to propose a methodology for assessing the security of information system assets. The methodology is based on a combination of a probabilistic approach to the analysis of possible scenarios for the implementation of threats in information systems for file system objects, expert assessments of basic attack events and representations in the form of attack trees. The threat implementation representation in the form of attack trees is used to simulate the actions of an attacker. **Results.** A structural model of an information system with cryptographic transformation of objects has been developed. Its valuable assets have been allocated. The list of the main threats to information security relevant for such systems is defined. Possible variants of the ways of implementing attacks and possible scenarios of the development of events in the processes of transferring file system objects with cryptographic transformation are modeled. A set of measures for the protection of information system objects with cryptographic transformation of objects is proposed. The calculation of the probabilities of attacks on an asset along the path determined by the attack tree, the possibility of implementing an attack, the degree of effectiveness of the proposed countermeasures is proposed. **Conclusion.** The presented methodology for assessing the security of an information system with cryptographic transformation of objects makes it possible to use well-known approaches in a comprehensive manner, and will be useful to developers and researchers in practical and scientific activities to ensure information security.

Keywords: security assessment, probabilistic approach, information protection, qualitative approach, attack trees

For citation: Artyushina L.A., Polyansky D.A. Approaches to assessing the security of information systems with cryptographic transformation of objects. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*. 2024;24(1):32–43. (In Russ.) DOI: 10.14529/ctcr240103

Введение

Применение информационных технологий в различных сферах деятельности человека, рост числа и масштабов информационных систем (ИС), активные действия злоумышленников, преследующих корыстные или деструктивные цели, поднимают задачу обеспечения уровня защищённости ИС на новый уровень [1–6]. Файловая система (ФС) является одним из компонентов ИС, особенно уязвимых к атакам злоумышленников, следовательно, повышение уровня защищённости ИС невозможно без обеспечения достаточного уровня защиты объектов ФС, атаки на которые затрагивают в том числе интересы пользователей ИС. Для принятия решений по использованию тех или иных механизмов защиты объектов ФС необходима регулярная оценка их текущего уровня защищённости с применением вероятностного подхода и деревьев атак для их моделирования, которые использованы в данной работе.

Введём необходимые рабочие определения и допущения. Вслед за [7] под ИС будем понимать совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств. Исходя из представления о базе данных как ресурсе с распределённым доступом, а также о том, что одним из наиболее эффективных способов обеспечения свойства конфиденциальности информации является её шифрование [8, 9], примем в качестве исследуемого варианта ИС систему с криптографическим преобразованием объектов ФС (ИСКПО). Такая система может быть построена, например, на известном алгоритме *CAST-128* с режимом *CBC*. А для полного сокрытия содержимого исходных данных и повышения криптоустойчивости передаваемой между клиентом и сервером информации в ИСКПО может быть использован алгоритм *AES-128* с повторным шифрованием данных. Принято допущение о том, что при расшифровании папки представляют собой файл.

Цель данной работы состоит в построении модели оценки защищённости ИСКПО в условиях применения злоумышленником широкого спектра атак на ФС.

Модель ИСКПО

Для реализации базовых функций управления доступом ИСКПО предоставляет пользователям возможности регистрации и авторизации под своей учётной записью, шифрования и расшифрования файлов и папок. Структурно ИСКПО можно описать совокупностью двух пакетов классов и объектов.

Пакет «Сервер»:

1) класс *стартовое окно сервера*: стартовоеОкно – отображает графический интерфейс; кнопкаАктивированииСервера – необходима для перехода к рабочему окну и непосредственной активации сервера;

2) класс *рабочее окно сервера*: рабочееОкно – отображает графический интерфейс;

3) класс *сервер*: активацияСервера – переводит сервер в рабочее состояние; взаимодействиеСКлиентом – необходим для взаимодействия с клиентом;

4) класс *БД*: проверитьНаличиеПользователя – проверка наличия пользователя в БД; проверитьНаличиеФайла – проверка наличия файла в БД; проверкаНаличияТаблицыПользователей – проверка наличия таблицы с пользователями в БД; проверкаНаличияТаблицыФайлов – проверка наличия таблицы файлов в БД; созданиеТаблицыПользователей – создание таблицы пользователей в БД; созданиеТаблицыФайлов – создание таблицы файлов в БД; добавитьДанныеПользователя – добавление данных зарегистрированного пользователя в БД; добавитьДанныеФайла – добавить данные зашифрованного файла в БД.

Пакет «Клиент»:

1) класс *Криптография*: шифрованиеБлочное – инициирует шифрование файла/папки на алгоритме *CAST-128*; расшифрованиеБлочное – инициирует расшифрование файла/папки на алгоритме *CAST-128*; генерацияСтартовыхПараметров – генерирует ключ и вектор, инициализации, идентификатор; созданиеХэша – преобразует входные данные в хэш; шифрованиеAES – шифрует данные для их отправления на сервер; расшифрование*AES* – расшифровывает данные сервера; прочитатьИдентификатор – считывает идентификатор из шифрованного фала;

2) класс *окно регистрации/авторизации*: кнопкаРегистрации – активирует регистрацию на основе информации, введённой пользователем; кнопкаАвторизации – осуществляет авторизацию на основе информации, введённой пользователем; отображениеОкнаВхода – отображает окно регистрации/авторизации;

3) класс *окно шифрования/расшифрования*: кнопкаШифрование – инициирует шифрование; кнопкаРасшифрование – инициирует расшифрование; отображениеОкнаРаботы – отображает окно шифрования/расшифрования;

4) класс *Архив*: архивация – осуществление архивации; рекурсивнаяАрхивация – рекурсивная архивация файлов и папок внутри каждой папки в папке; созданиеФайлаАрхива – создание непосредственно файла архива;

5) класс *Клиент*: обменИнформацией – осуществляет обмен информацией с сервером.

Структура пакетов «Сервер» и «Клиент» представлена на рис. 1 и 2.

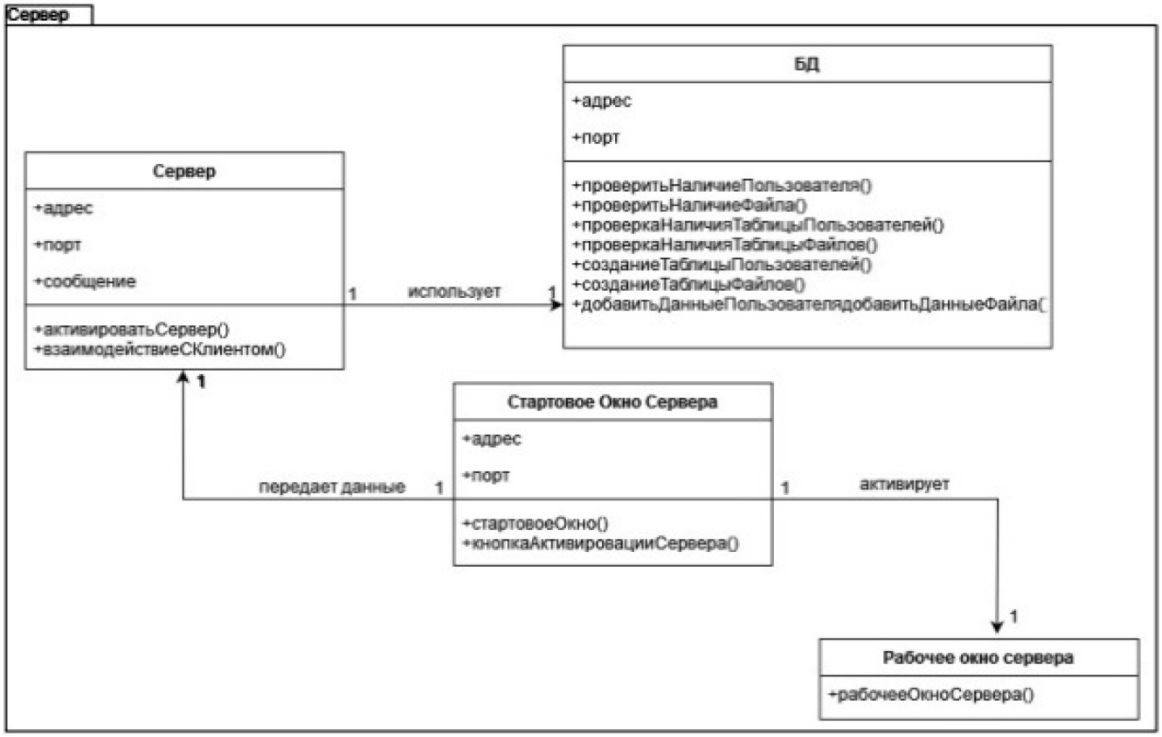

Рис. 1. Пакет «Сервер»
Fig. 1. The "Server" Package

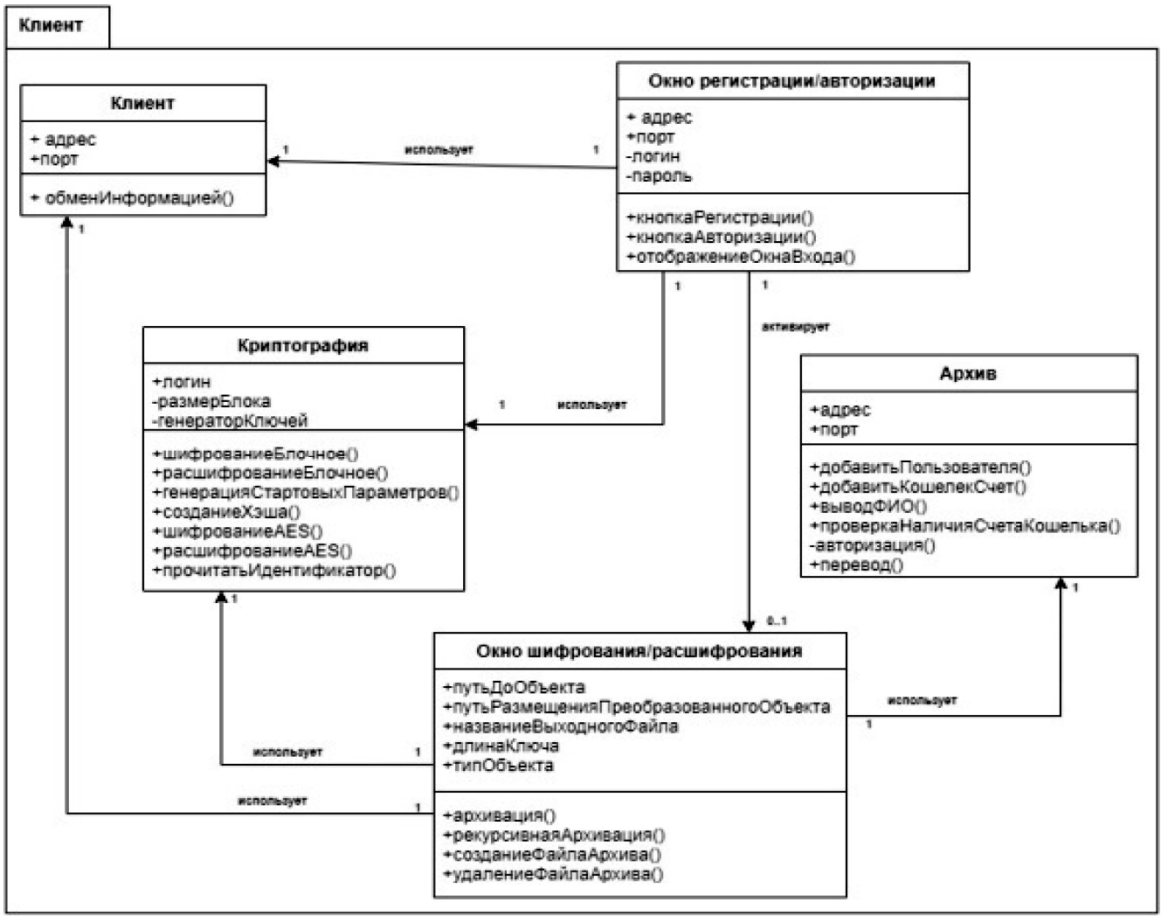

Рис. 2. Пакет «Клиент»
Fig. 2. The "Client" package

При шифровании папок пользователь должен предварительно преобразовать их в архив, который на следующем шаге будет зашифрован и предоставлен пользователю. Используемый в работе алгоритм шифрования относится к блочным шифрам и предполагает обработку данных блоками фиксированной длины. Эта особенность определила структуру базы данных (БД), используемой в ИСКПО:

$$\begin{cases} \text{ИСКПО} = \langle U, FI \rangle; \\ U = \langle Log_i, Pass_i \rangle,\ i = 1..n; \\ FI = \langle ID_j, Vec_j, Ost_j, Len_j, Km_j, Kr_j \rangle,\ j = 1..k, \end{cases} \quad (1)$$

где U – множество пользователей;

FI – множество данных, характеризующих шифрованные файлы.

$$U = \langle Log_i, Pass_i \rangle,\ i = 1..n, \quad (2)$$

где Log_i – логин i-го пользователя;

$Pass_i$ – пароль i-го пользователя;

n – количество пользователей в системе.

$$FI = \langle ID_j, Vec_j, Ost_j, Len_j, Km_j, Kr_j \rangle,\ j = 1..k, \quad (3)$$

где ID_j – идентификатор j-го файла, является хешированной зашифрованной последовательностью первых 64 000 бит данных;

Vec_j – вектор инициализации j-го файла, используется для предотвращения повторного шифрования данных, что усложняет процесс взлома;

Ost_j – остаток в блоке j-го файла, образуется, если последний используемый блок данных некратен размеру блока, в этом случае последний блок дополняется случайными цифрами предпоследнего байта;

Len_j – длина ключа j-го файла. Алгоритм шифрования *CAST-128* позволяет варьировать длину ключа в диапазоне от 40 до 128 бит, в нашем случае $Len_j = 128$ как позволяющая реализовывать алгоритм на большинстве современных платформ [9];

Km_j, Kr_j – части ключа j-го файла, в алгоритме используются как маскировка ключа и перестановки ключа соответственно;

k – количество данных, характеризующих шифрованные файлы.

Подробно использованный алгоритм шифрования описан в [9].

Разработка перечня угроз информационной безопасности (ИБ) активам ИСКПО

ИСКПО полностью соответствует определению ИС, данному в Федеральном законе N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [7], поэтому можно выделить следующие основные активы ИСКПО:

− информационные ресурсы: база данных, траффик ($Y1$);

− аппаратное обеспечение: сервер, оперативная память ($Y2$).

За рамки работы вынесены вопросы защиты сетевого оборудования и программной среды как относящиеся к обязанностям администратора безопасности. Основным моделируемым процессом в ИСКПО является защита файла путём его шифрования. Анализ с использованием БД УБИ ФСТЭК [10] позволяет выявить следующие актуальные угрозы ИСПО, представленные в табл. 1.

Таблица 1

Угрозы ИСКПО и пути их реализации

Table 1

Threats of lawsuits and ways of their implementation

№	Название угрозы	Код актива	Пути реализации угрозы
1	Угроза длительного удержания вычислительных ресурсов пользователями	*Y1*	Многократные обращения к серверу различных клиентов
2	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	*Y1*	Постоянное многократное обращение к серверу с одного клиента
3	Угроза избыточного выделения оперативной памяти	*Y2*	Шифрование файла огромного размера (равного объёму оперативной памяти)
4	Угроза неправомерного ознакомления с защищаемой информацией	*Y1*	Хищение БД
5	Угроза несанкционированного доступа к аутентификационной информации	*Y1, Y2*	Чтение информации из БД
6	Угроза несанкционированного копирования защищаемой информации	*Y2*	Копирование БД
7	Угроза использования слабостей протоколов сетевого/локального обмена данными	*Y1*	Чтение сетевого трафика
8	Угроза перехвата данных, передаваемых по вычислительной сети	*Y1, Y2*	Модификация сетевого трафика
9	Угроза ошибочной аутентификации	*Y1,Y2*	Подбор аутентификационных данных

Оценка возможности атак на ИСКПО

Принятие решений по управлению механизмами ИБ и выбор тех или иных средств защиты основаны на оценке рисков для ИС, которая носит вероятностный характер [11–14]. Оценка вероятности реализации атак на ИСКПО в данной работе основана на ранжировании угроз ИБ в результате анализа функционирования системы на некотором промежутке времени *T*. Этот период можно охарактеризовать количеством и типом реализованных атак на активы ИС.

Можно выделить основные свойства потока событий типа «атака» для ИСКПО:

− поток стационарен ввиду того, что к ИСКПО применимо требование круглосуточной доступности сервисов, что даёт возможность злоумышленникам осуществить попытку реализации угрозы в любое время;

− практика показывает [5], что на одну ИС направлены различные атаки вне зависимости от результативности более ранних атак, поток обладает свойством отсутствия последействия;

− поток ординарен, поскольку в основе ИСКПО лежит защищаемая локальная сеть организации и вероятность появления более одной атаки за малый промежуток времени пренебрежимо мала по сравнению с вероятностью появления в системе одного такого события.

Данные свойства позволяют сделать вывод о том, что поток событий типа «атака» для ИСКПО удовлетворяет основным свойствам простейшего потока Пуассона и интенсивность атак подчиняется закону распределения Пуассона [11], и вероятность того, что за время *T* произойдёт именно *k* атак определённого типа при среднем числе атак λ на данном интервале времени *T*, равна

$$p(k) = \frac{\lambda^k}{k!} \cdot e^{-\lambda}. \quad (4)$$

Вслед за [6] введём допущение, разделив инциденты по нескольким категориями, объединив угрозы в группы по способу реализации:

1) эксплуатация уязвимости: угроза длительного удержания вычислительных ресурсов пользователями, угроза избыточного выделения оперативной памяти;

2) угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов, угроза несанкционированного копирования защищаемой информации;

3) компрометация учётной записи: угроза неправомерного ознакомления с защищаемой информацией, угроза несанкционированного доступа к аутентификационной информации; угроза ошибочной аутентификации;

4) сетевые атаки: угроза использования слабостей протоколов сетевого/локального обмена данными, угроза перехвата данных, передаваемых по вычислительной сети, угроза использования слабостей протоколов сетевого/локального обмена данными.

Поскольку функционал моделируемой ИСКПО изначально не предусматривает работу в web (система не использует web-приложения), то web-атаки, равно как и внедрение заражённого ПО и т. п., также вынесены за рамки работы.

В первом приближении для ранжирования угроз по ожидаемой вероятности их реализации (p_i) может быть использована шкала баллов:

$$\begin{cases} \text{1-й ранг – высокая вероятность угрозы, } p_i \geq 0{,}1; \\ \text{2-й ранг – средняя вероятность угрозы, } 0{,}05 \leq p_i < 0{,}1; \\ \text{3-й ранг – низкая вероятность угрозы, } p_i < 0{,}05. \end{cases}$$

Оценка ожидаемых вероятностей реализации угроз основана на статистическом распределении инцидентов с разным и высоким уровнями критичности [6]:

$$p_c = \frac{p_{d3}+p_{d4}+p_{h3}+p_{h4}}{n}, \quad (5)$$

где p_c – среднее значение вероятности; p_{d3}, p_{d4} – вероятности инцидентов с разным уровнем критичности за III, IV кварталы 2022 года; p_{h3}, p_{h4} – вероятности инцидентов с высоким уровнем критичности за III, IV кварталы 2022 года; n – количество месяцев в III, IV кварталах 2022 года. Результаты расчётов по категориям угроз представлены в табл. 2.

Таблица 2

Значения вероятности реализации угроз (по категориям)

Table 2

Probability values for threats to materialize (by category)

№	Категории угроз	Вероятность реализации угроз	Ранг угроз
1	Эксплуатация уязвимости	0,07	2
2	Компрометация учетной записи	0,04	3
3	Сетевые атаки	0,03	3

Поскольку атака – это реализация угрозы, в качестве базовых событий (вариантов атак) можно принять выделенные выше угрозы.

Подходы и методы оценки вероятностей базовых событий являются задачами дополнительных исследований. В работе для такой оценки была использована комбинированная методика, включающая в себя экспертные оценки и вероятностный подход к анализу рисков безопасности и оценке эффективности систем защиты [14, 15]. Введём следующие параметры и их градации:

1) S – сложность атаки: а) 1 – реализация атаки не требует усилий; б) 2 – атаку просто реализовать; в) 3 – атака сложна в реализации;

2) C – стоимость атаки: а) 1 – атака низкой стоимости; б) 2 – атака средней стоимости; в) 3 – атака высокой стоимости;

3) L – сложность обнаружения атаки: а) 1 − атаку сложно обнаружить; б) 2 – атаку достаточно сложно обнаружить; в) 3 – атаку легко обнаружить;

4) K_1 – возможность возникновения источника события, K_2 – степень готовности источника события, K_3 – ущерб от реализации события: 1–2 – очень низкая(ий), 3–4 – низкая(ий), 5–7 – средняя(ий), 8–9 – высокая(ий), 10 – очень высокая(ий).

В выборе параметров можно руководствоваться соображениями целесообразности проведения атаки. Значениями параметров являются экспертные оценки, выставляемые в ходе проводимых тестов на проникновение, позволяющие выявить проблемы в архитектуре ИСКПО, конфигурации сервера. Пример характеристик базовых событий в соответствии с приведёнными параметрами и их градациями представлен в табл. 3.

Таблица 3

Пример характеристик базовых событий

Table 3

Example of characteristics of basic events

№	Базовые события	S	C	L	K_1	K_2	K_3
1	Длительное удержание вычислительных ресурсов	2	1	3	3	10	5
2	Неконтролируемый рост числа зарезервированных вычислительных ресурсов	2	1	3	3	10	5
3	Избыточное выделение оперативной памяти	2	1	3	1	10	3
4	Неправомерное ознакомление с защищаемой информацией	3	2	2	7	10	7
5	Несанкционированный доступ к аутентификационной информации	3	2	2	7	10	7
6	Угроза несанкционированного копирования защищаемой информации	3	2	1	7	10	7
7	Использование слабостей протоколов сетевого/локального обмена данными	2	1	3	7	10	7
8	Перехват данных, передаваемых по вычислительной сети	1	1	3	7	10	7
9	Ошибочная аутентификация	3	2	3	5	10	4

С учётом значимости входных параметров вероятность базового события равна:

$$p = w_1 \cdot u(S) + w_2 \cdot u(C) + w_3 \cdot u(L), \quad (6)$$

где w_1, w_2, w_3 – нормированные весовые коэффициенты, обозначающие значимость каждого входного параметра для итогового результата, $\sum_1^3 w_i = 1$.

Оценка весовых коэффициентов также является предметом дополнительных исследований. В первом приближении сложность атаки, стоимость атаки и сложность обнаружения атаки можно принять равными в оценке её целесообразности:

$w_1 = w_2 = w_3 = 1/3$,

Функция преобразования:

$$u(x) = \frac{c}{x}, \quad (7)$$

где c – коэффициент преобразования.

Для коэффициента преобразования принято следующее допущение: при минимальных оценках всех базовых событий вероятность основного события должна попадать под определение высокой вероятности успешности атаки. В данном случае использовано значение $c = 0{,}3$. Расчет вероятностей базовых событий представлен ниже. Нумерация вероятностей соответствует табл. 3.

$$p_1 = p_2 = p_3 = p_7 = \frac{0{,}3}{3}\left(\frac{1}{2} + \frac{1}{1} + \frac{1}{3}\right) = 0{,}18;$$

$$p_4 = p_5 = \frac{0{,}3}{3}\left(\frac{1}{3} + \frac{1}{2} + \frac{1}{2}\right) = 0{,}13;$$

$$p_6 = p_7 = \frac{0{,}3}{3}\left(\frac{1}{3} + \frac{1}{2} + \frac{1}{1}\right) = 0{,}18;$$

$$p_8 = \frac{0{,}3}{3}\left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3}\right) = 0{,}18;$$

$$p_9 = \frac{0{,}3}{3}\left(\frac{1}{3} + \frac{1}{2} + \frac{1}{3}\right) = 0{,}12.$$

Комплекс контрмер

Для нейтрализации угроз ИБ применительно к активам ИСКПО предложен комплекс контрмер, включающий в себя как хорошо известные меры защиты ИС, так и учитывающие особенности моделируемой ИСКПО, представленный в табл. 4.

Таблица 4

Контрмеры

Table 4

Countermeasures

№ базового события	Контрмеры
1	Паузы после каждого обращения клиента к серверу в течение 5 секунд. Блокировка функционала клиента (возможности запускать шифрование и расшифрование), во время криптографических преобразований
2	Паузы после каждого обращения клиента к серверу в течение 5 секунд. Блокировка функционала клиента (возможности запускать шифрование и расшифрование) во время криптографических преобразований
3	Шифрование фиксированных блоков данных из файла
4	Данные в БД хранятся в шифрованном и хешированном виде, в зависимости от таблиц
5	Данные в БД хранятся в шифрованном и хешированном виде, в зависимости от таблиц
6	Данные в БД хранятся в шифрованном и хешированном виде, в зависимости от таблиц
7	Передача хешированных (в случае логина и пароля) и шифрованных сообщений (в случаях иной информации)
8	Передача хешированных (в случае логина и пароля) и шифрованных сообщений (в случаях иной информации)
9	Паузы после каждого обращения клиента к серверу, 5 секунд после первого обращение и далее по +1 секунда от времени каждого предыдущего обращения

Применение методологии деревьев атак в модели управления ИБ ИСКПО

Деревья атак являются формальным методом моделирования реализации угроз ИБ в отношении ИС. Атаки представляются в виде деревьев, где корень – цель атаки, ближайшие узлы – подцели атаки, листья – способы достижения подцелей и реализации атаки на основную цель. Узлы в дереве могут быть типа «И» и «ИЛИ». Для реализации атаки необходимо обойти все дочерние узлы типа «И» или хотя бы один узел типа «ИЛИ». Подробно методология деревьев атак и её применение представлены в работах [1–5]. Рассмотрим использование методологии деревьев атак для моделирования и обнаружения инцидентов ИБ в модели ИСКПО на примере одной угрозы. Для каждой угрозы были определены цель и возможные варианты атаки, основанные на описании угроз и путях их реализации (см. табл. 1, 4).

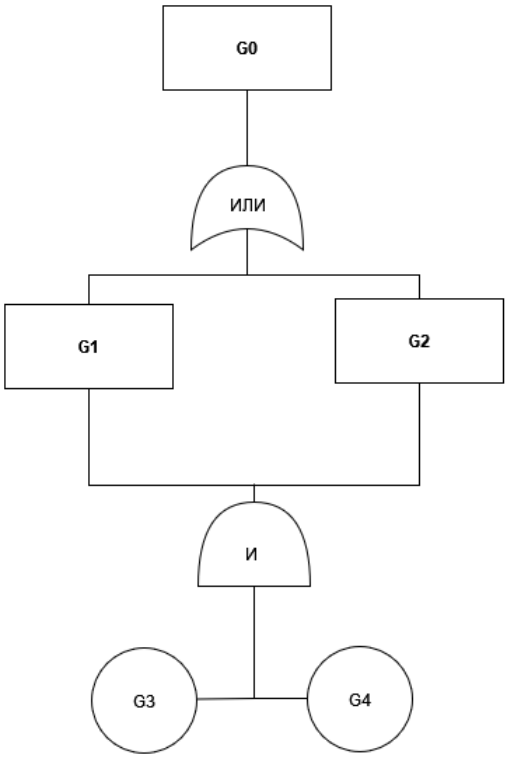

Рис. 3. Дерево атак на сервер
Fig. 3. The Tree of attacks on the server

Угроза 1: цель (*G*0) – сервер, варианты атаки: *G*1 – постоянное многократное обращение к серверу с одного клиента, *G*2 – многократные обращения к серверу различных клиентов.

Контрмеры: *G*3 – паузы после каждого обращения клиента к серверу в течение 5 секунд, *G*4 – блокировка функционала клиента (возможности запускать шифрование и расшифрование) во время криптографических преобразований. Дерево атак на сервер представлено на рис. 3.

Оценка эффективности предлагаемого комплекса контрмер

В первом приближении (при условии достоверной и полной оценки вероятностей базовых событий) эффективность мер защиты может быть рассчитана как вероятность состояния системы, при котором отсутствует источник атаки, он не готов к реализации события, а системе не нанесён ущерб от реализации события [14, 15]:

$$\delta_i = 1 - p_i \cdot \frac{K_1 \cdot K_2 \cdot K_3}{10^3}, \quad (8)$$

где δ_i – эффективность i-й контрмеры.

Расчёт эффективности контрмер (в соответствии с нумерацией табл. 4):

$\delta_1 = \delta_2 = 1 - 0{,}18 \cdot 0{,}15 = 0{,}973$;

$\delta_3 = 1 - 0{,}18 \cdot 0{,}03 = 0{,}995$;

$\delta_6 = \delta_7 = \delta_8 = 1 - 0{,}18 \cdot 0{,}49 = 0{,}936$;

$\delta_9 = 1 - 0{,}12 \cdot 0{,}2 = 0{,}976$.

Эффективность защиты для всех событий превышает 90 %, что свидетельствует об эффективности разработанного комплекса контрмер.

Заключение

В статье рассмотрена методика оценки защищённости информационной системы с криптографическим преобразованием файловых объектов, позволяющая смоделировать возможные варианты путей реализации атак и возможные сценарии развития событий в процессах передачи объектов файловой системы с криптографическим преобразованием, а также рассчитать вероятности реализации атак на актив по пути, определённому деревом атак, и степень эффективности предлагаемых контрмер. Методика даёт возможность комплексного применения известных подходов к оценке защищённости, будет полезна разработчикам и исследователям при выборе общих мер защиты информационных систем. Оценка возможностей реализации атак и эффективности мер защиты, учитывающая специфические особенности реализации ИСКПО, равно как и более широкого класса ИС, требует дальнейших исследований.

Работа выполнена во Владимирском государственном университете имени Александра Григорьевича и Николая Григорьевича Столетовых.

Список литературы

1. Алпеев Е.В., Стадник А.Н., Скрыль С.В. Методика прогнозирования компьютерных атак на основе определения весов атрибутов компьютерной атаки с применением метода деревьев решений // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2021. № 6. С. 82–92. ISSN: 2306-1456.

2. Кляус Т.К., Гатчин Ю.А. Определение вероятности реализации атак на информационную систему с помощью деревьев событий // Вестник УрФО. Безопасность в информационной сфере. 2018. № 4 (30). С. 31–37. DOI: 10.14529/secur180405, ISSN: 2225-5435.

3. Дородников Н.А. Разработка методики повышения уровня защищённости вычислительных сетей на основе вероятностной поведенческой модели, использующей деревья атак: дис. … канд. техн. наук: 05.13.19. СПб.: С.-Петерб. нац. исслед. ун-т информац. технологий, механики и оптики, 2017. 185 с.

4. Середкин М.Д., Атомян А.С., Моргунов В.М. Классификация компьютерных атак на основе деревьев решений // Методы и технические средства обеспечения безопасности информации. 2019. № 28. С. 107–108. ISSN: 2305-994X.

5. Чечулин А.А. Построение и анализ деревьев атак на компьютерные сети с учетом требования оперативности: дис. … канд. техн. наук: 05.13.19. СПб.: С.-Петерб. ин-т информатики и автоматизации РАН, 2013. 152 с.

6. Отчет о кибератаках на российские компании в 2022 году // Ростелеком Солар: сайт. URL: https://rt-solar.ru/analytics/reports/3332/ (дата обращения: 10.04.2023).

7. Российская Федерация. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ // КонсультантПлюс: сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 10.04.2023).

8. Спиричева Н.Р. Алгоритмы блочной криптографии. Екатеринбург: Изд-во Урал. ун-та, 2013. 78 с.

9. Гатченко Н.А., Исаев А.С., Яковлев А.Д. Криптографическая защита информации. СПб.: НИУ ИТМО, 2012. 142 с.

10. Федеральная служба по техническому и экспортному контролю (ФСТЭК России): сайт. URL: http://fstec.ru (дата обращения: 10.04.2023).

11. Вентцель Е.С., Овчаров Л.А. Теория вероятностей и ее инженерные приложения. М.: Высш. шк., 2000. 480 с.

12. Солодов А.К. Основы финансового риск-менеджмента. М.: Издание Александра К. Солодова, 2017. 286 с.

13. Linets G.I., Melnikov S.V. Criterion for identification of the probability model of the state of satellite communication channels // Современная наука и инновации. 2020. № 2 (30). С. 29–36.

14. Буй П.М. Оценка рисков кибербезопасности инфокоммуникационных систем // Вестник Белорусского государственного университета транспорта: наука и транспорт. 2020. № 2 (41). С. 20–23.

15. Пашков Н.Н., Дрозд В.Г. Анализ рисков информационной безопасности и оценка эффективности систем защиты информации на предприятии // Современные научные исследования и инновации. 2020. № 1 [Электронный ресурс]. URL: https://web.snauka.ru/issues/2020/01/90380 (дата обращения: 10.04.2023).

References

1. Alpeyev E.V., Stadnik A.N., Skryl S.V. A method of predicting computer attacks based on determining the weights of attributes of a computer attack using the decision tree method. Electronic network polythematic journal “Scientific Works of the Kuban State Technological University”. 2021;6:82–92. (In Russ.) ISSN: 2306-1456.

2. Klyaus T.K., Gatchin Yu.A. Probability evaluation of attacks on information system using event tree analysis. Journal of the Ural Federal district. Information security. 2018;4(30):31–37. (In Russ.) DOI: 10.14529/secur180405, ISSN: 2225-5435.

3. Dorodnikov N.A. *Razrabotka metodiki povysheniya urovnya zashchishchënnosti vychislitel’nykh setey na osnove veroyatnostnoy povedencheskoy modeli, ispol’zuyushchey derev’ya atak: dis. kand. tekhn. nauk: 05.13.19* [Development of a technique for increasing the level of security of computer networks based on a probabilistic behavioral model using attack trees. Cand. sci. diss.]. St. Petersburg: St. Petersburg National Research University of Information Technologies, Mechanics and Optics; 2017. 185 p. (In Russ.)

4. Seredkin M.D., Atomyan A.S., Morgunov V.M. [Classification of computer attacks based on decision trees]. *Metody i tekhnicheskiye sredstva obespecheniya bezopasnosti informatsii*. 2019;28:107–108. (In Russ.) ISSN: 2305-994X.

5. Chechulin A.A. *Postroyeniye i analiz derev’yev atak na komp’yuternyye seti s uchetom trebovaniya operativnosti: dis. kand. tekhn. nauk: 05.13.19* [Construction and analysis of attack trees on computer networks, taking into account the requirements of efficiency. Cand. sci. diss.]. St. Petersburg: St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences; 2013. 152 p. (In Russ.)

6. *Otchet o kiberatakakh na rossiyskie kompanii v 2022 godu* [Report on cyber attacks on Russian companies in 2022]. *Rostelekom Solar: website*. (In Russ.) Available at: https://rt-solar.ru/analytics/reports/3332/ (accessed 10.04.2023).

7. *Rossiyskaya Federatsiya. Federal'nyy zakon “Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii” ot 27.07.2006 N 149-FZ* [Russian Federation. Federal Law “On Information, Information Technologies and Information Protection” dated July 27, 2006 N 149-FZ]. *Konsul'tantPlyus: website*. (In Russ.) Available at: https://www.consultant.ru/document/cons_doc_LAW_61798/ (accessed 10.04.2023).

8. Spiricheva N.R. *Algoritmy blochnoy kriptografii* [Block cryptography algorithms]. Ekaterinburg: Ural University Publ; 2013. 78 p. (In Russ.)

9. Gatchenko N.A., Isaev A.S., Yakovlev A.D. *Kriptograficheskaya zashchita informatsii* [Cryptographic protection of information]. St. Petersburg: ITMO University; 2012. 142 p. (In Russ.)

10. *Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu (FSEK Rossii): sayt* [Federal Service for Technical and Export Control (FSTEC of Russia): website]. (In Russ.) Available at: http://fstec.ru (accessed 10.04.2023).

11. Venttsel' E.S., Ovcharov L.A. *Teoriya veroyatnostey i ee inzhenernye prilozheniya* [Probability theory and its engineering applications]. Moscow: Vysshaya shkola; 2000. 480 p. (In Russ.)

12. Solodov A.K. *Osnovy finansovogo risk-menedzhmenta* [Fundamentals of financial risk management]. Moscow: Edition of Alexander K. Solodov; 2017. 286 p. (In Russ.)

13. Linets G.I., Melnikov S.V. Sriterion for identification of the probability model of the state of satellite communication channels. *Modern Science and Innovations*. 2020;2(30):29–36.

14. Bui P.M. Assessment of the cybersecurity risks infocommunication's systems of railway transport. *Bulletin of the Belarusian State University of Transport: science and transport*. 2020;2(41):20–23. (In Russ.)

15. Pashkov N.N., Drozd V.G. [Analysis of information security risks and assessment of the effectiveness of information security systems at the enterprise]. *Modern scientific researches and innovations*. 2020;1. (In Russ.) Available at: https://web.snauka.ru/issues/2020/01/90380 (accessed 10.04.2023).

Информация об авторах

Артюшина Лариса Андреевна, канд. пед. наук, магистр направления «Информационные системы и технологии», доц. кафедры информатики и защиты информации, Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Владимир, Россия; larisa-artusina@yandex.ru.

Полянский Дмитрий Александрович, канд. техн. наук, доц. кафедры информатики и защиты информации, Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Владимир, Россия; polyansk@rambler.ru.

Information about the authors

Larisa A. Artyushina, Cand. Sci. (Education), Master's degree in Information Systems and Technologies, Ass. Prof. of the Department of Informatics and Information Protection, Vladimir State University named after Alexander and Nicolay Stoletovs, Vladimir, Russia; larisa-artusina@yandex.ru.

Dmitry A. Polyansky, Cand. Sci. (Eng.), Ass. Prof. of the Department of Informatics and Information Protection, Vladimir State University named after Alexander and Nicolay Stoletovs, Vladimir, Russia; polyansk@rambler.ru.

Статья поступила в редакцию 12.10.2023
The article was submitted 12.10.2023