МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 34

ОТЧЕТ   
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| доцент, к.э.н. |  |  |  | Т.Н. Елина |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |
| ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №1 | | | | |
| ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ МОДЕЛИ С ПОЛНЫМ ПЕРЕКРЫТИЕМ УГРОЗ | | | | |
| по курсу: МЕТОДОЛИГИЯ ЗАЩИТЫ ИНФОРМАЦИИ | | | | |

РАБОТУ ВЫПОЛНИЛИ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТЫ ГР. № | 3843 |  |  |  | Калинина А.С,  Конева А.П., Шумков Е.Г. |
|  |  |  | подпись, дата |  | инициалы, фамилия |

Санкт-Петербург 2021

1. **Цель работы**: исследование возможностей графового моделирования для анализа рисков информационной безопасности, изучение принципов построения двудольных и трехдольных графов с полным перекрытием множества угроз безопасности.
2. **Задачи**: провести системный анализ выбранной предметной области (организации). На основании полученных данных выделить множества объектов защиты и угроз информационной безопасности, построить двудольный граф. Разработать методы защиты информации, построить трехдольный граф. Проанализировать полученные результаты.

Информационная безопасность — это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудования, предназначенных для использования. В связи с развитием информационных технологий и компьютеризацией экономики одним из важнейших вопросов в деятельности любой компании становится обеспечение информационной безопасности.

При выполнении лабораторной работы в качестве организации была выбрана нотариальная контора.

Нотариальное делопроизводство регламентируется Приказом Минюста России от 16.04.2014 № 78 «Об утверждении Правил нотариального делопроизводства». Согласно данному документу, нотариус и нотариальные палаты являются операторами персональных данных. Обработка персональных данных осуществляется нотариусом в обязательном порядке при установлении личности обратившегося для совершения нотариального действия лица, внесении записей в реестр при регистрации нотариального действия.

План помещения организации представлен на рисунке 1.

Рисунок 1 — План помещения организации

В кабинете нотариуса расположены рабочее место (включая персональный компьютер) нотариуса, место для совершения нотариальных сделок, рабочий сейф. В данном сейфе хранятся организационно — распорядительные документы, к которым относятся приказы и распоряжения (согласно ч.2 Приказа Минюста России № 78 от 16.04.2014 года), а также печати с воспроизведением Государственного герба Российской Федерации, штампы, бланки и усиленная квалифицированная электронная подпись нотариуса (ч.5 Приказа Минюста России № 78 от 16.04.2014 года). Кроме того, в этом кабинете находится рабочее место старшего помощника нотариуса, который занимается ведением реестров регистрации нотариальных действий (ч.12 Приказа Минюста России № 78 от 16.04.2014 года), заполнением книг специального учета (например, учета наследственных дел, учета завещаний), обработкой писем, к которым относятся ответы на запросы, информационные сообщения, справки, уведомления и т.д.

В серверной расположен сервер, к которому подключены персональные компьютеры нотариуса и помощников и на котором хранится документация в электронном виде.

В архиве расположены картотеки номенклатурных дел (ч. 6, 7, 8 Приказа Минюста России № 78 от 16.04.2014 года), а также личные дела сотрудников организации и копии документов в печатном виде.

Помощники нотариусов принимают документы у клиентов (их оригиналы или копии) и подготавливают всю необходимую для совершения нотариальной сделки документацию.

Объект защиты информации — это информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

При выполнении лабораторной работы было выделено множество О — множество объектов защиты, состоящее из следующих элементов:

* + 1. О1 – сервер;
    2. О2 — персональный компьютер нотариуса;
    3. О3 — персональные компьютеры помощников;
    4. О4 — Сейф;
    5. О5 — Картотека номенклатурных дел (в печатном виде расположена в архиве, в электронном — на сервере);
    6. О6 — Персональные данные сотрудников (в архиве находится картотека личных дел, на сервере — электронные копии);
    7. О7 — Персональные данные клиентов (оригиналы или копии документов);
    8. О8 — Книги специального учета, реестры и письма (располагаются в кабинете нотариуса возле рабочего места старшего помощника).

Угрозы информационной безопасности — это совокупность условий и факторов, создающих опасность нарушения информационной безопасности, это различные действия, которые могут привести к нарушениям состояния защиты информации.

Выделяем множество угроз У информационной безопасности в рамках рассматриваемой организации, состоящее из следующих элементов:

У1 – физическое воздействие(замыкание)

У2 – несанкционированное копирование данных

У3 – несанкционированное удаление данных или их модификация

У4 – заражение вредоносным ПО через внешний носитель

У5 – заражение вредоносным ПО через сеть

У6 – DDoS атака на сервер

У7 – несанкционированный доступ к трафику и его перехват

У8 – чтение или фотографирование информации с экрана ПК

У9 – несанкционированное распечатывание электронной версии документа

У10 – повреждение замка или стенок сейфа с использованием вспомогательных инструментов

У11 – попытка взлома сейфа с использованием подбора пароля

У12 – несанкционированное копирование бумажных данных

У13 – кража бумажных документов

У14 – уничтожение бумажных носителей

У15 – разглашение сотрудниками конфиденциальной информации

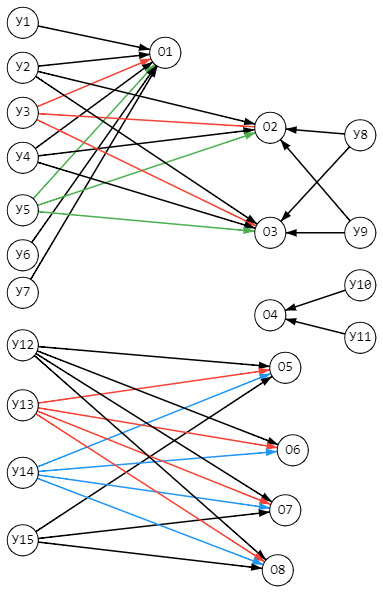
Множество отношений «объект — угроза» образуют двудольный граф, приведенный на рисунке 2.

Рисунок 2 — Двудольный граф

Рассчитали примерную вероятность осуществления угроз и стоимость ущерба, который может понести организация в случае их осуществления. Данные занесены в Таблицу 1.

Таблица №1. Результаты расчетов вероятности угроз и стоимости ущерба

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № угрозы | Вероятность P | Стоимость ущерба,  тыс. руб. | Описание ущерба | Итог  (PxC)  тыс. руб. |
| 1 | 0,05 | 85 | Стоимость нового оборудования + половина зарплаты помощника нотариуса за месяц = 65+20 | 4,25 |
| 2 | 0,37 | 750 | Штраф за разглашение конфиденциальной информации(150) + упущенная выгода в случае приостановления действия лицензии на месяц (600) | 277,5 |
| 3 | 0,23 | 123,5 | Потеря информации критической важности, фактически остановка работы конторы + услуги системного администратора (3,5) + упущенная выгода на 3 дня (120) | 28,405 |
| 4 | 0,6 | 203,5 | Требуется много времени на восстановление информации, упущенная выгода на неделю (200) + услуги системного администратора (3,5) | 122,1 |
| 5 | 0,7 | 203,5 | Требуется много времени на восстановление информации, упущенная выгода на неделю (200) + услуги системного администратора (3,5) | 142,45 |
| 6 | 0,02 | 3,5 | услуги системного администратора (3,5) | 0,07 |
| 7 | 0,01 | 3,5 | услуги системного администратора (3,5) | 0,035 |
| 8 | 0,64 | 750 | Штраф за разглашение конфиденциальной информации(150) + упущенная выгода в случае приостановления действия лицензии на месяц (600) | 480 |
| 9 | 0,25 | 750 | Штраф за разглашение конфиденциальной информации(150) + упущенная выгода в случае приостановления действия лицензии на месяц (600) | 187,5 |
| 10 | 0,04 | 440 | Стоимость нового сейфа (40) + упущенная прибыль на время восстановление гербовой печати (400) | 17,6 |
| 11 | 0,1 | 440 | Стоимость нового сейфа (40) + упущенная прибыль на время восстановление гербовой печати (400) | 44 |
| 12 | 0,4 | 750 | Штраф за разглашение конфиденциальной информации(150) + упущенная выгода в случае приостановления действия лицензии на месяц (600) | 300 |
| 13 | 0,35 | 750 | Штраф за разглашение конфиденциальной информации(150) + упущенная выгода в случае приостановления действия лицензии на месяц (600) | 262,5 |
| 14 | 0,15 | 770 | В случае восстановления с электронной версии: половина зарплаты помощника нотариуса за 2 недели(20) + Штраф за разглашение конфиденциальной информации(150) + упущенная выгода в случае приостановления действия лицензии на месяц (600) | 115,5 |
| 15 | 0,03 | 750 | Штраф за разглашение конфиденциальной информации(150) + упущенная выгода в случае приостановления действия лицензии на месяц (600) | 22,5 |

Модель системы безопасности с полным перекрытием угроз — это наиболее общая модель защиты автоматизированных систем, базирующаяся на том, что система безопасности должна иметь по крайне мере одно средство, обеспечивающее безопасность любого потенциального канала утечки информации. В модели точно определяется каждая область, требующая защиты, оцениваются средства обеспечения безопасности с точки зрения их эффективности и их вклад в обеспечение безопасности во всей вычислительной системе.

Методы и способы защиты информации подразумевают применение конкретных мер и технологий, позволяющих решать проблемы в области обеспечения информационной безопасности предприятий и ведомств.

Выделяем множество М, включающее в себя следующие методы защиты:

m11 – доступ в помещение путем отпирания механического дверного замка и отпирания электромагнитного замка путем прикладывания ID карты к считывателю СКУД (системы контроля управления доступом) / установка системы видеонаблюдения/ внедрение пожарной сигнализации и средств пожаротушения/ система охранной сигнализации для помещения

m21 – аутентификация по SSH для доступа к серверу / использование ID-карты для аутентификации пользователя/ система охранной сигнализации для помещения

m31 – использование ID-карты для аутентификации пользователя/ периодическое создание бэкапа архива документов (напр. с использованием RAID-массивов) / аудит файлов с использованием системы обнаружения и предотвращения вторжений (IDS/IPS)/ система охранной сигнализации для помещения

m41 – запрет использования сотрудниками внешних носителей, не предусмотренных первоначальной комплектацией / использование антивирусного ПО/ периодическое создание бэкапа архива документов

m51 – использование антивирусного ПО/ периодическое создание бэкапа документации

m61 – установка файрвола (брандмауэра)

m71 – установка файрвола (брандмауэра)

m22 – использование ID-карты для аутентификации пользователя/ использование программного средства защиты информации от НСД (напр. «Снег-2.0») для контроля использования защищаемой информации и выявления попыток несанкционированного доступа к защищаемой информации/ система охранной сигнализации для помещения

m32 – использование ID-карты для аутентификации пользователя/ периодическое создание бэкапа архива документов/ аудит файлов с использованием системы обнаружения и предотвращения вторжений (IDS/IPS)/ система охранной сигнализации для помещения/ использование ID-карты для аутентификации пользователя

m42 – запрет использования сотрудниками внешних носителей, не предусмотренных первоначальной комплектацией / использование антивирусного ПО / установка системы видеонаблюдения/ периодическое создание бэкапа архива документов

m52 – использование антивирусного ПО/ периодическое создание бэкапа документации

m82 – использование ID-карты для аутентификации пользователя / использование защитной пленки на стеклах окон

m92 – печать с автоматической маркировкой каждой страницы и автоматическим оформлением учетной карточки документа с указанием даты печати, учетных реквизитов, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности, фамилии лица, выдавшего документ, количества страниц и копий документа/ использование ID-карты для аутентификации пользователя

m23 – использование ID-карты для аутентификации пользователя / использование программного средства защиты информации от НСД (напр. «Снег-2.0») для контроля использования защищаемой информации и выявления попыток несанкционированного доступа к защищаемой информации/ система охранной сигнализации для помещения

m33 – использование ID-карты для аутентификации пользователя/ периодическое создание бэкапа архива документов/ аудит файлов с использованием системы обнаружения и предотвращения вторжений (IDS/IPS)/ система охранной сигнализации для помещения

m43 – запрет использования сотрудниками внешних носителей, не предусмотренных первоначальной комплектацией / использование антивирусного ПО/ периодическое создание бэкапа архива документов

m53 – использование антивирусного ПО/ периодическое создание бэкапа документации

m83 – использование ID-карты для аутентификации пользователя / использование защитной пленки на стеклах окон

m93 – печать с автоматической маркировкой каждой страницы и автоматическим оформлением учетной карточки документа с указанием даты печати, учетных реквизитов, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности, фамилии лица, выдавшего документ, количества страниц и копий документа/ использование ID-карты для аутентификации пользователя

m10-4 – использование нескольких видов замков одновременно (напр. механический и электронный) и дополнительной дверцы (трейзера)/ система охранной сигнализации для помещения

m11-4 – установка охранной сигнализации для сейфа/ система охранной сигнализации для помещения/ установка системы видеонаблюдения

m12-5 - доступ в помещение по ID-карте / установка механических замков на дверцы шкафчика с документацией/ установка системы видеонаблюдения

m13-5 - доступ в помещение по ID-карте / периодическое создание бэкапа архива документов/ установка механических замков на дверцы шкафчика с документацией/ установка системы видеонаблюдения/ система охранной сигнализации для помещения

m14-5 - доступ в помещение по ID-карте / периодическое создание бэкапа архива документов/ установка механических замков на дверцы шкафчика с документацией/ установка системы видеонаблюдения / внедрение пожарной сигнализации и средств пожаротушения/ система охранной сигнализации для помещения

m15-5 - инструктаж сотрудников по ИБ/ обеспечение конфиденциальности данных путем заключения соглашения о неразглашении конфиденциальных данных сотрудниками

m12-6 - доступ в помещение по ID-карте / установка механических замков на дверцы шкафчика с документацией/ установка системы видеонаблюдения

m13-6 - доступ в помещение по ID-карте / установка системы видеонаблюдения/ периодическое создание бэкапа архива документов/ установка механических замков на дверцы шкафчика с документацией/ установка системы видеонаблюдения/ система охранной сигнализации для помещения

m14-6 - доступ в помещение по ID-карте / периодическое создание бэкапа архива документов/ установка механических замков на дверцы шкафчика с документацией/ установка системы видеонаблюдения/ внедрение пожарной сигнализации и средств пожаротушения/ система охранной сигнализации для помещения

m12-7 - доступ в помещение по ID-карте / установка механических замков на дверцы шкафчика с документацией/ установка системы видеонаблюдения

m13-7 - доступ в помещение по ID-карте / установка системы видеонаблюдения/ периодическое создание бэкапа архива документов/ установка механических замков на дверцы шкафчика с документацией/ установка системы видеонаблюдения/ система охранной сигнализации для помещения

m14-7 - доступ в помещение по ID-карте / периодическое создание бэкапа архива документов/ установка механических замков на дверцы шкафчика с документацией/ установка системы видеонаблюдения/ внедрение пожарной сигнализации и средств пожаротушения/ система охранной сигнализации для помещения

m15-7 - инструктаж сотрудников по ИБ/ обеспечение конфиденциальности данных путем заключения соглашения о неразглашении конфиденциальных данных сотрудниками

m12-8 - доступ в помещение по ID-карте / установка механических замков на дверцы шкафчика с документацией/ установка системы видеонаблюдения

m13-8 - доступ в помещение по ID-карте / периодическое создание бэкапа архива документов/ установка механических замков на дверцы шкафчика с документацией/ установка системы видеонаблюдения/ система охранной сигнализации для помещения

m14-8 - доступ в помещение по ID-карте / периодическое создание бэкапа архива документов/ установка механических замков на дверцы шкафчика с документацией/ установка системы видеонаблюдения/ внедрение пожарной сигнализации и средств пожаротушения/ система охранной сигнализации для помещения

m15-8 - инструктаж сотрудников по ИБ/ обеспечение конфиденциальности данных путем заключения соглашения о неразглашении конфиденциальных данных сотрудниками

Набор средств обеспечения безопасности преобразует двудольный граф в трехдольный, представленный на рисунке 3. Ребра указывают на соответствующие связи между угрозами, методами защиты и множеством объектов защиты.

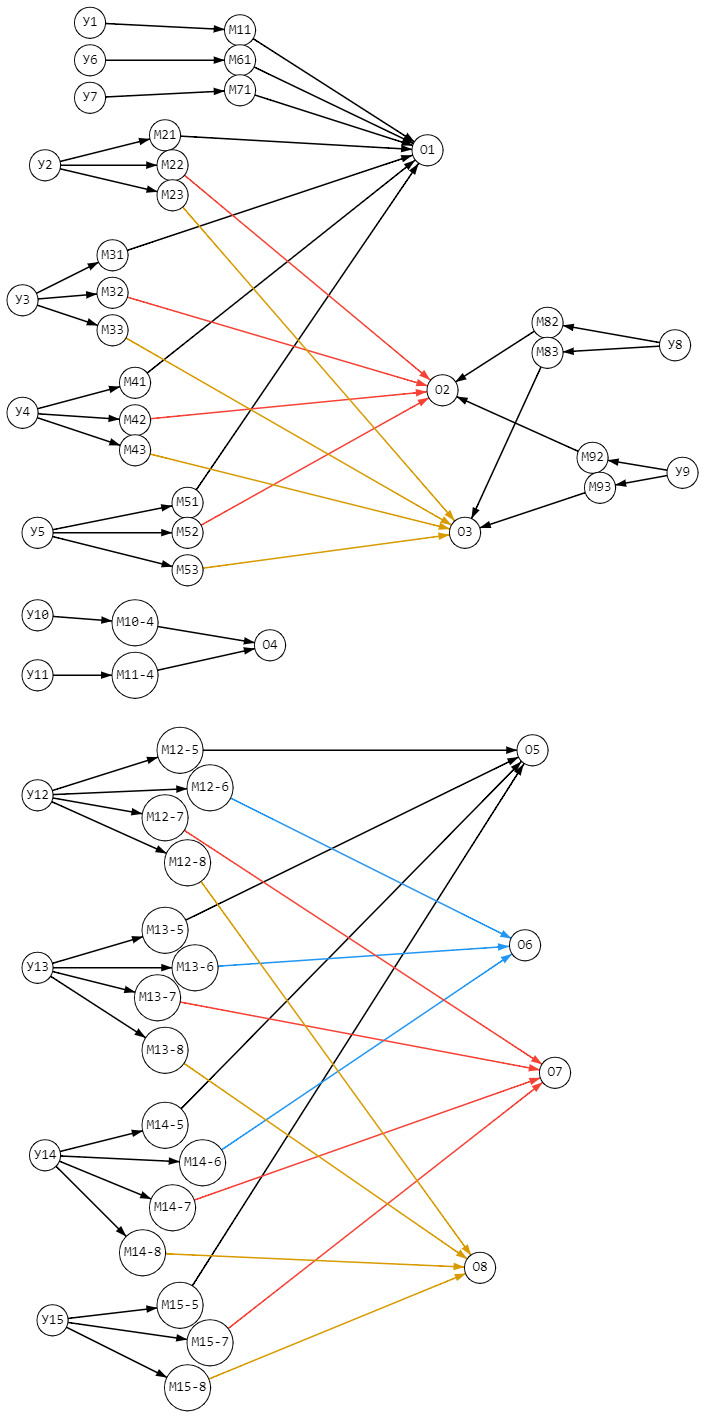


Рисунок 3 — Трехдольный граф

Проанализировав полученный граф, можно выделить наиболее универсальные методы защиты информации. К ним относятся:

m1- использование ID-карты для аутентификации пользователя

m2- периодическое создание бэкапа архива документов

m3- использование антивирусного ПО/ установка файрвола

m4- установка системы видеонаблюдения

m5 - установка механических замков на дверцы шкафчика с документацией

m6- доступ в помещение путем отпирания механического дверного замка и отпирания электромагнитного замка путем прикладывания ID карты к считывателю СКУД (системы контроля управления доступом)

m7- запрет использования сотрудниками внешних носителей, не предусмотренных первоначальной комплектацией

m8- печать с автоматической маркировкой каждой страницы и автоматическим оформлением учетной карточки документа с указанием даты печати, учетных реквизитов, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности, фамилии лица, выдавшего документ, количества страниц и копий документа

m9- внедрение пожарной сигнализации и средств пожаротушения

m10- система охранной сигнализации для помещения

m11- инструктаж сотрудников по ИБ/ обеспечение конфиденциальности данных путем заключения соглашения о неразглашении конфиденциальных данных сотрудниками

m12 - использование защитной пленки на стеклах окон

На основе этих методов получаем упрощенный трехдольный граф, изображенный на рисунке 4.

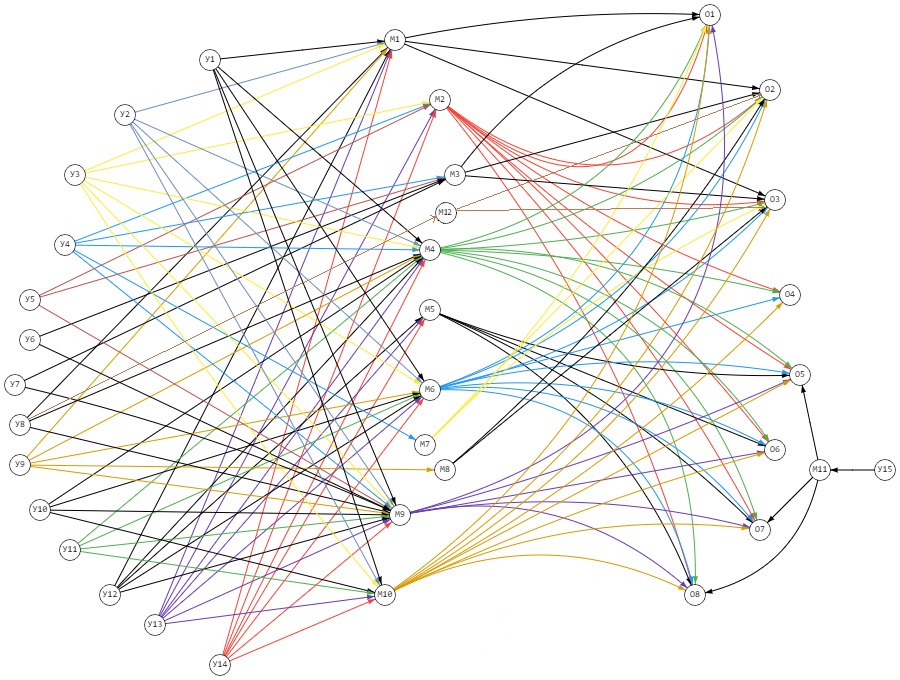


Рисунок 4 — Упрощенный трехдольный граф

Рассчитали суммарную стоимость убытков в результате осуществления угроз и затраты на введение конкретных методов защиты, сравнили полученные данные, сделали вывод о рациональности внедрения данных методов защиты информации. Результаты отображены в Таблице №2.

Таблица №2. Сравнение стоимости внедрения и суммарной стоимости ущерба

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Метод | Стоимость внедрения, тыс. руб. | Описание | ∑Стоимость ущерба , тыс. руб. | Вывод |
| m1 | 22 | Считыватели СКУД (10)+ ID-карты(6) + работа по установке считывателей(6) | 1655,7 | Целесообразно |
| m2 | 11,5 | Услуги системного администратора (1,5) + стоимость новых жестких дисков (10) | 520,5 | Целесообразно |
| m3 | 31 | Настройка файрвола(1) + Kaspersky расширенная версия для бизнеса(30) | 246,7 | Целесообразно |
| m4 | 25 | Установка системы видеонаблюдения | 1839,4 | Целесообразно |
| m5 | 4 | Работа по установке механических замков + замки | 678,0 | Целесообразно |
| m6 | 22 | Считыватели СКУД + ID-карта + работа по установке считывателей | 1237,3 | Целесообразно |
| m7 | 5 | Проведение обучающего инструктажа по ИБ | 122,1 | Целесообразно |
| m8 | 2 | Настройка необходимого ПО | 187,5 | Целесообразно |
| m9 | 27 | Установка системы пожарной сигнализации(20)+ огнетушители(7) | 119,8 | Целесообразно |
| m10 | 20 | Установка системы охранной сигнализации | 749,8 | Целесообразно |
| m11 | 5 | Проведение обучающего инструктажа по ИБ | 22,5 | Целесообразно |
| m12 | 5 | Использование защитной пленки на стеклах окон | 480 | Целесообразно |

Сравнив полученные значения стоимости внедрения перечисленных методов и стоимости ущерба в результате осуществления угроз, можно сделать вывод, что внедрение данных методов является целесообразным, поскольку затраты на внедрение не превышают стоимости ущерба.

**Вывод**

На основании проведенного системного анализа на примере нотариальной конторы, план помещения которой воспроизведен на рисунке 1, выделили множество объектов защиты О, состоящее из следующих элементов: О1 – сервер; О2 — персональный компьютер нотариуса; О3 — персональные компьютеры помощников; О4 — Сейф; О5 — Картотека номенклатурных дел (в печатном виде расположена в архиве, в электронном — на сервере); О6 — Персональные данные сотрудников (в архиве находится картотека личных дел, на сервере — электронные копии); О7 — Персональные данные клиентов (оригиналы или копии документов); О8 — Книги специального учета, реестры и письма (располагаются в кабинете нотариуса возле рабочего места старшего помощника).

Также выделили множество угроз У информационной безопасности из 15 элементов: У1 – физическое воздействие(замыкание), У2 – несанкционированное копирование данных, У3 – несанкционированное удаление данных или их модификация, У4 – заражение вредоносным ПО через внешний носитель, У5 – заражение вредоносным ПО через сеть, У6 – DDoS атака на сервер, У7 – несанкционированный доступ к трафику и его перехват, У8 – чтение или фотографирование информации с экрана ПК, У9 – несанкционированное распечатывание электронной версии документа, У10 – повреждение замка или стенок сейфа с использованием вспомогательных инструментов, У11 – попытка взлома сейфа с использованием подбора пароля, У12 – несанкционированное копирование бумажных данных, У13 – кража бумажных документов , У14 – уничтожение бумажных носителей, У15 – разглашение сотрудниками конфиденциальной информации. Исходя из полученных данных построили двудольный граф вида «угроза-объект», отображенный на рисунке 2. Рассчитали примерную вероятность осуществления угроз и стоимость ущерба, который может понести организация в случае их осуществления (Таблица №1).

Разработали методы защиты информации, выделив множество методов М. Поскольку набор средств обеспечения безопасности преобразует двудольный граф в трехдольный, построили трехдольный граф, представленный на рисунке 3.

Проанализировав полученный граф, выделили и перечислили 12 наиболее универсальных методов защиты информации. На основе этих методов получили упрощенный трехдольный граф, изображенный на рисунке 4. Рассчитав суммарную стоимость убытков в результате осуществления угроз и затраты на введение конкретных методов защиты (Таблица №2), сделали вывод о целесообразности внедрения рассматриваемых методов защиты информации m1 - m12.

Рассмотренная модель безопасности с полным перекрытием угроз применима, в основном, как инструментарий при разработке определенных политик безопасности либо в случае построения комплексной защиты информации для малого предприятия, так как при больших множествах объектов защиты информации, угроз информационной безопасности и методов защиты анализ модели становится затруднительным.

**Список литературы:**

1. Информационная безопасность – Режим доступа: <https://pirit.biz/reshenija/informacionnaja-bezopasnost>
2. Приказ Минюста России от 16.04.2014 № 78 «Об утверждении Правил нотариального делопроизводства» – Режим доступа: <http://www.consultant.ru/document/cons_doc_LAW_162343/>
3. Объекты защиты информации – Режим доступа: <https://intuit.ru/studies/courses/3649/891/lecture/32324>
4. Угрозы информационной безопасности – Режим доступа: [https://ru.wikipedia.org/wiki/%D0%A3%D0%B3%D1%80%D0%BE%D0%B7%D1%8B\_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9\_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8](https://ru.wikipedia.org/wiki/Угрозы_информационной_безопасности)
5. Модель системы безопасности с полным перекрытием – Режим доступа: [https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C\_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B\_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8\_%D1%81\_%D0%BF%D0%BE%D0%BB%D0%BD%D1%8B%D0%BC\_%D0%BF%D0%B5%D1%80%D0%B5%D0%BA%D1%80%D1%8B%D1%82%D0%B8%D0%B5%D0%BC](https://ru.wikipedia.org/wiki/Модель_системы_безопасности_с_полным_перекрытием)
6. Методы и способы защиты информации – Режим доступа: [https://www.anti-malware.ru/practice/methods#:~:text=%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D1%8B%20%D0%B8%20%D1%81%D0%BF%D0%BE%D1%81%D0%BE%D0%B1%D1%8B%20%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%8B%20%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8%20%D0%BF%D0%BE%D0%B4%D1%80%D0%B0%D0%B7%D1%83%D0%BC%D0%B5%D0%B2%D0%B0%D1%8E%D1%82%20%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%BA%D0%BE%D0%BD%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D1%8B%D1%85%20%D0%BC%D0%B5%D1%80%20%D0%B8,%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9%20%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8%20%D0%BF%D1%80%D0%B5%D0%B4%D0%BF%D1%80%D0%B8%D1%8F%D1%82%D0%B8%D0%B9%20%D0%B8%20%D0%B2%D0%B5%D0%B4%D0%BE%D0%BC%D1%81%D1%82%D0%B2](https://www.anti-malware.ru/practice/methods#:~:text=Методы%20и%20способы%20защиты%20информации%20подразумевают%20применение%20конкретных%20мер%20и,информационной%20безопасности%20предприятий%20и%20ведомств).