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 №2 | | | | |
| КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ АКТИВОВ | | | | |
| 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**: провести анализ информационных ресурсов компании и выработать предложения по обеспечению корпоративной информационной безопасности.
2. **Задачи**: провести системный анализ выбранной предметной области (организации). На основании полученных данных выделить информационные активы. Провести классификацию информационных активов. Выделить наиболее опасные каналы утечки информации, разработать способы противодействия утечке информации. Проанализировать полученные результаты.

В качестве организации в рамках данной лабораторной работы рассматривается нотариальная контора, сотрудниками которой являются: нотариус, старший помощник, помощники и системный администратор (по контракту с аутсорсинговой компанией).

Информационный актив – информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для организации, находящаяся в распоряжении организации и представленная на любом материальном носителе в пригодном для ее обработки, хранения и передачи форме.

Информационные активы должны иметь ценность для организации, их нельзя заменить без затрат каких – либо ресурсов, они оказывают ценность на деятельность организации. На основании этих критериев были выделены следующие информационные активы: учетно – отчетная документация (включает в себя книги специального учета, реестры), персональные данные сотрудников, персональные данные клиентов, номенклатурные дела, сведения о техническом состоянии ЭВМ, информация о заключенных нотариальных сделках, необходимая для регистрации в книгах специального учета и реестрах, доверенности, позволяющие помощникам заключать сделки, проводить консультации от имени нотариуса, распоряжения и поручения.

На рисунке 1 представлено, как используются информационные ресурсы в рамках нотариальной конторы.

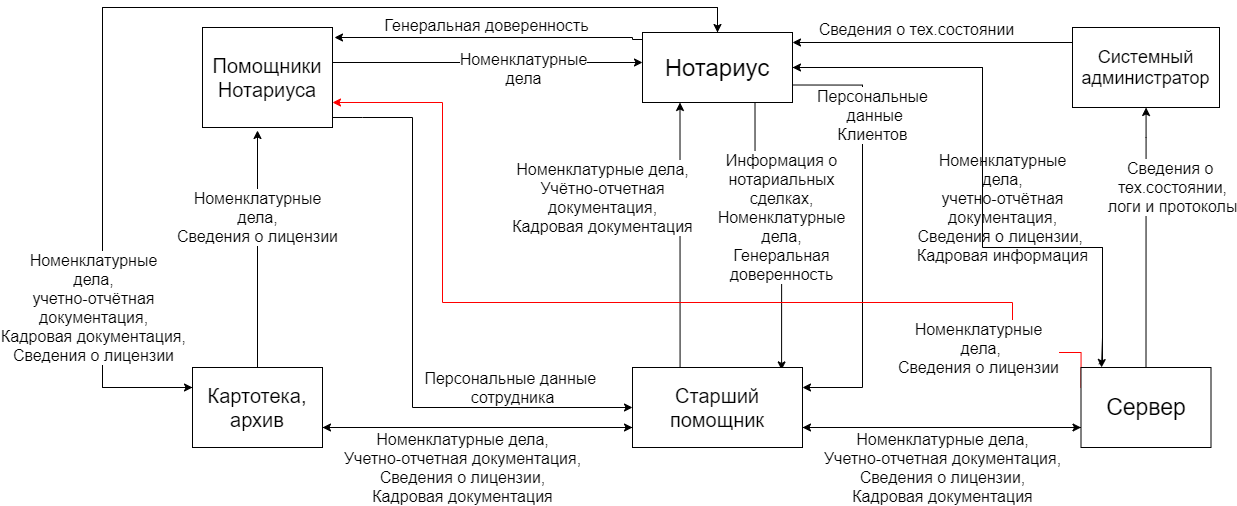


Рисунок 1 - Схема информационных активов

Классификация информационных активов – разделение существующих информационных активов по типам, выполняемая в соответствии со степенью тяжести последствия от потери их значимых свойств информационной безопасности.

Для классификации информационных активов по шкалам значимости обеспечения конфиденциальности, целостности, доступности, определения типа информации, а также владельцев и пользователей была составлена таблица 1. При этом шкала значимости определена в диапазоне от 1 до 5 (1 – не высокая важность, 5 – максимальное значение).

Таблица 1. Классификация информационных активов

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Название группы ИА | Описание | Формат | Размещение | | Класс | | | Тип | Владелец | Пользователь |
| Физическое | ИС | К | Ц | Д |
| 1 | Учетно -отчетная документация | Служебная отчетная документация (книги спец.учета, реестры) | Бумажный и электронный | Кабинет нотариуса  (место старшего помощника) | «Информационная система нотариуса «еНот» на сервере | 3 | 3 | 2 | КТ | Старший помощник | Старший помощник, нотариус |
| 2 | Персональные данные сотрудников | Паспортные данные, банковские реквизиты, контактные данные | Бумажный и электронный | Картотека личных дел в архиве | «Информационная система нотариуса «еНот» на сервере | 4 | 3 | 2 | ПД | Картотека, сервер | Старший помощник, нотариус |
| 3 | Персональные данные клиентов | Оригиналы и копии документов, контактные данные | Бумажный и электронный | Картотека личных дел в архиве | «Информационная система нотариуса «еНот» на сервере | 5 | 5 | 4 | ПД | Картотека, сервер | Старший помощник, нотариус, помощники |
| 4 | Номенклатурные дела | Нотариально – оформленные сделки и документы по ним | Бумажный и электронный | Картотека номенклатурных дел в архиве | «Информационная система нотариуса «еНот» на сервере | 5 | 3 | 5 | КТ | Картотека, сервер | Нотариус, помощники |
| 5 | Сведения о техническом состоянии ЭВМ | Заключения системного администратора, автоматические отчеты ЭВМ | Электронный | - | Файлы на сервере, лог-журналы | 1 | 1 | 1 | Открытая | Сервер | Нотариус,  системный администратор |
| 6 | Информация о нотариальных сделках | Сведения для регистрации в реестрах и книгах учета | Бумажный и электронный | Кабинет нотариуса  (место старшего помощника) | Электронные письма | 5 | 4 | 3 | КТ | Нотариус | Старший помощник |
| 7 | Доверенности | Разрешение на осуществление деятельности (заключение сделок, осуществление консультаций) от имени лица (нотариуса) | Бумажный | Кабинеты нотариуса  (место старшего помощника), кабинеты помощников | - | 2 | 5 | 4 | ПД | Нотариус | Старший помощник, помощники |
| 8 | Распоряжения и поручения | Приказы помощникам | Электронный | - | «Информационная система нотариуса «еНот» на сервере | 1 | 3 | 4 | КТ | Нотариус | Старший помощник, помощники |
| 9 | Кадровая информация | Личные дела сотрудников, карточки по учёту кадров, приказы о движении персонала | Бумажный и электронный | Кабинет нотариуса  (место старшего помощника) | «Информационная система нотариуса «еНот» на сервере | 3 | 3 | 2 | КТ | Старший помощник | Старший помощник, нотариус |
| 10 | Сведения о лицензии | Лицензия на осуществление деятельности | Бумажный и Электронный | Кабинет нотариуса,  сейф | Файл на сервере | 1 | 3 | 3 | Открытая | Сервер | Нотариус,  Старший помощник,  Помощники |

Единая информационная система нотариата РФ (еНот) состоит из следующих информационных блоков: нотариусы, нотариальные палаты, образцы печатей и подписей, бланки единого образца, отмененные доверенности, сведения о завещаниях, аресты, сведения о недействительных документах, наследственные дела и т.д. Кроме того, она позволяет вести отчетность и статистику, создавать архивы документов, осуществлять электронный документооборот.

Существуют различные виды информации и виды тайн: открытая информация; персональные данные; информация, содержащая сведения, составляющие банковскую тайну; информация, содержащая сведения, составляющие коммерческую тайну. В соответствии с этой классификацией информационные активы были распределены по видам тайн, а также определено число пользователей данных информационных активов и носители информации. Результаты представлены в таблице 2.

Таблица 2 – Виды и разновидности тайн

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вид тайны | Информационные активы | ИС | Число пользователей | Носители информации |
| КТ | Учетно-отчетная информация | «Информационная система нотариуса «еНот» на сервере | Старший помощник – 1  Нотариус - 1 | Бумажные и электронные носители |
| ПД | Персональные данные сотрудников | «Информационная система нотариуса «еНот» на сервере | Старший помощник – 1  Нотариус - 1 | Бумажные и электронные носители |
| ПД | Персональные данные клиентов | «Информационная система нотариуса «еНот» на сервере | Старший помощник – 1  Нотариус – 1  Помощники - 2 | Бумажные и электронные носители |
| КТ | Номенклатурные дела | «Информационная система нотариуса «еНот» на сервере | Старший помощник – 1  Нотариус - 1 | Бумажные и электронные носители |
| Открытая | Сведения о техническом состоянии ЭВМ | Файлы, лог-журналы | Нотариус – 1  Системный администратор - 1 | Электронные файлы и лог-журналы |
| КТ | Информация о нотариальных сделках | «Информационная система нотариуса «еНот» на сервере | Старший помощник - 1 | Бумажные и электронные носители |
| ПД | Доверенности | - | Старший помощник -1  Помощники - 2 | Бумажные носители |
| КТ | Распоряжения и поручения | «Информационная система нотариуса «еНот» на сервере | Старший помощник -1  Помощники - 2 | Электронные носители |
| КТ | Кадровая информация | «Информационная система нотариуса «еНот» на сервере | Старший помощник – 1  Нотариус - 1 | Бумажные и электронные носители |
| Открытая | Сведения о лицензии | Файл на сервере | Старший помощник – 1  Нотариус - 1  Помощники - 2 | Бумажные и электронные носители |

Утечка информации – это неконтролируемое распространение информации за пределы организации, помещения, здания, какой – либо территории, а также определенного круга лиц, которые имеют доступ к этой информации. Защита от утечки информации требует проведения обязательных организационных и технических мер, которые позволяют выявить вероятные каналы утечки и предотвратить несанкционированное распространение информации.

В результате анализа информационных активов организации, способов их использования и хранения, а также списка владельцев и пользователей были выявлены наиболее опасные и вероятные каналы утечки информации, а также разработана система средств и мер противодействия. Результаты представлены в таблице 3.

Таблица 3 – Оценка рисков информационной безопасности

|  |  |  |  |
| --- | --- | --- | --- |
| № | Информационные активы | Наиболее опасные каналы утечки информации | Способы противодействия утечке |
|  | Учетно-отчетная информация | Несанкционированное копирование, удаление, модификация данных на сервере | Доступ в помещение по ID-карте/ установка системы видеонаблюдения/установка системы охранной сигнализации/аутентификация по SSH для доступа к серверу/ периодическое создание бэкапа/аудит файлов с помощью IDS/IPC/запрет использования сотрудниками внешних носителей/использование антивирусного ПО и файрвола/использование программного средства защиты информации от НСД. |
| Чтение или фотографирование информации с экранов ПК компьютеров сотрудников | Использование защитной пленки на стеклах окон/проведение обучающего инструктажа по ИБ/ использование системы Screen Guard |
| Несанкционированное распечатывание электронной версии документа | Печать с автоматической маркировкой каждой страницы и автоматическим оформлением учётной карточки документа с указанием даты печати, учётных реквизитов, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности, фамилии лица, выдавшего документ, количества страниц и копий документа. |
| Несанкционированное копирование бумажных носителей | 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 |
| Кража бумажных носителей | 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 |
| Уничтожение бумажных носителей (пожар) | 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 |
| Разглашение данных сотрудниками организации | Инструктаж сотрудников по ИБ/ обеспечение конфиденциальности данных путем заключения соглашения о неразглашении конфиденциальных данных сотрудниками |
| Физическое воздействие на сервер | 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 |
| Заражение вредоносным ПО | Использование антивирусного ПО/ установка файрвола/ запрет использования сотрудниками внешних носителей, не предусмотренных первоначальной комплектацией / периодическое создание бэкапа архива документов/ установка системы видеонаблюдения |
| Использование нелицензированного ПО | Приобретение и установка лицензированного ПО |
|  | Персональные данные сотрудников | Несанкционированное копирование, удаление, модификация данных на сервере | Доступ в помещение по ID-карте/ установка системы видеонаблюдения/установка системы охранной сигнализации/аутентификация по SSH для доступа к серверу/ периодическое создание бэкапа/аудит файлов с помощью IDS/IPC/запрет использования сотрудниками внешних носителей/использование антивирусного ПО и файрвола/использование программного средства защиты информации от НСД. |
| Чтение или фотографирование информации с экранов ПК компьютеров сотрудников | Использование защитной пленки на стеклах окон/проведение обучающего инструктажа по ИБ/ использование системы Screen Guard |
| Несанкционированное распечатывание электронной версии документа | Печать с автоматической маркировкой каждой страницы и автоматическим оформлением учётной карточки документа с указанием даты печати, учётных реквизитов, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности, фамилии лица, выдавшего документ, количества страниц и копий документа. |
| Несанкционированное копирование бумажных носителей | 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 |
| Кража бумажных носителей | 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 |
| Уничтожение бумажных носителей (пожар) | 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 |
| Разглашение данных сотрудниками организации | Инструктаж сотрудников по ИБ/ обеспечение конфиденциальности данных путем заключения соглашения о неразглашении конфиденциальных данных сотрудниками |
| Физическое воздействие на сервер | 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 |
| Заражение вредоносным ПО | Использование антивирусного ПО/ установка файрвола/ запрет использования сотрудниками внешних носителей, не предусмотренных первоначальной комплектацией / периодическое создание бэкапа архива документов/ установка системы видеонаблюдения |
| Использование нелицензированного ПО | Приобретение и установка лицензированного ПО |
|  | Персональные данные клиентов | Несанкционированное копирование, удаление, модификация данных на сервере | Доступ в помещение по ID-карте/ установка системы видеонаблюдения/установка системы охранной сигнализации/аутентификация по SSH для доступа к серверу/ периодическое создание бэкапа/аудит файлов с помощью IDS/IPC/запрет использования сотрудниками внешних носителей/использование антивирусного ПО и файрвола/использование программного средства защиты информации от НСД. |
| Чтение или фотографирование информации с экранов ПК компьютеров сотрудников | Использование защитной пленки на стеклах окон/проведение обучающего инструктажа по ИБ/ использование системы Screen Guard |
| Несанкционированное распечатывание электронной версии документа | Печать с автоматической маркировкой каждой страницы и автоматическим оформлением учётной карточки документа с указанием даты печати, учётных реквизитов, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности, фамилии лица, выдавшего документ, количества страниц и копий документа. |
| Несанкционированное копирование бумажных носителей | 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 |
| Кража бумажных носителей | 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 |
| Уничтожение бумажных носителей (пожар) | 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 |
| Разглашение данных сотрудниками организации | Инструктаж сотрудников по ИБ/ обеспечение конфиденциальности данных путем заключения соглашения о неразглашении конфиденциальных данных сотрудниками |
| Физическое воздействие на сервер | 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 |
| Заражение вредоносным ПО | Использование антивирусного ПО/ установка файрвола/ запрет использования сотрудниками внешних носителей, не предусмотренных первоначальной комплектацией / периодическое создание бэкапа архива документов/ установка системы видеонаблюдения |
| Использование нелицензированного ПО | Приобретение и установка лицензированного ПО |
|  | Номенклатурные дела | Несанкционированное копирование, удаление, модификация данных на сервере | Доступ в помещение по ID-карте/ установка системы видеонаблюдения/установка системы охранной сигнализации/аутентификация по SSH для доступа к серверу/ периодическое создание бэкапа/аудит файлов с помощью IDS/IPC/запрет использования сотрудниками внешних носителей/использование антивирусного ПО и файрвола/использование программного средства защиты информации от НСД. |
| Чтение или фотографирование информации с экранов ПК компьютеров сотрудников | Использование защитной пленки на стеклах окон/проведение обучающего инструктажа по ИБ/ использование системы Screen Guard |
| Несанкционированное распечатывание электронной версии документа | Печать с автоматической маркировкой каждой страницы и автоматическим оформлением учётной карточки документа с указанием даты печати, учётных реквизитов, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности, фамилии лица, выдавшего документ, количества страниц и копий документа. |
| Несанкционированное копирование бумажных носителей | 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 |
| Кража бумажных носителей | 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 |
| Уничтожение бумажных носителей (пожар) | 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 |
| Разглашение данных сотрудниками организации | Инструктаж сотрудников по ИБ/ обеспечение конфиденциальности данных путем заключения соглашения о неразглашении конфиденциальных данных сотрудниками |
| Физическое воздействие на сервер | 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 |
| Заражение вредоносным ПО | Использование антивирусного ПО/ установка файрвола/ запрет использования сотрудниками внешних носителей, не предусмотренных первоначальной комплектацией / периодическое создание бэкапа архива документов/ установка системы видеонаблюдения |
| Использование нелицензированного ПО | Приобретение и установка лицензированного ПО |
|  | Сведения о техническом состоянии ЭВМ | Физическое воздействие на сервер | 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 |
| Несанкционированное копирование, удаление, модификация данных на сервере | Доступ в помещение по ID-карте/ установка системы видеонаблюдения/установка системы охранной сигнализации/аутентификация по SSH для доступа к серверу/ периодическое создание бэкапа/аудит файлов с помощью IDS/IPC/запрет использования сотрудниками внешних носителей/использование антивирусного ПО и файрвола/использование программного средства защиты информации от НСД |
| Заражение вредоносным ПО | Использование антивирусного ПО/ установка файрвола/ запрет использования сотрудниками внешних носителей, не предусмотренных первоначальной комплектацией / периодическое создание бэкапа архива документов/ установка системы видеонаблюдения |
|  | Информация о нотариальных сделках | Несанкционированное копирование, удаление, модификация данных на сервере | Доступ в помещение по ID-карте/ установка системы видеонаблюдения/установка системы охранной сигнализации/аутентификация по SSH для доступа к серверу/ периодическое создание бэкапа/аудит файлов с помощью IDS/IPC/запрет использования сотрудниками внешних носителей/использование антивирусного ПО и файрвола/использование программного средства защиты информации от НСД. |
| Чтение или фотографирование информации с экранов ПК компьютеров сотрудников | Использование защитной пленки на стеклах окон/проведение обучающего инструктажа по ИБ/ использование системы Screen Guard |
| Несанкционированное распечатывание электронной версии документа | Печать с автоматической маркировкой каждой страницы и автоматическим оформлением учётной карточки документа с указанием даты печати, учётных реквизитов, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности, фамилии лица, выдавшего документ, количества страниц и копий документа. |
| Несанкционированное копирование бумажных носителей | 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 |
| Кража бумажных носителей | 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 |
| Уничтожение бумажных носителей (пожар) | 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 |
| Разглашение данных сотрудниками организации | Инструктаж сотрудников по ИБ/ обеспечение конфиденциальности данных путем заключения соглашения о неразглашении конфиденциальных данных сотрудниками |
| Физическое воздействие на сервер | 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 |
| Заражение вредоносным ПО | Использование антивирусного ПО/ установка файрвола/ запрет использования сотрудниками внешних носителей, не предусмотренных первоначальной комплектацией / периодическое создание бэкапа архива документов/ установка системы видеонаблюдения |
| Использование нелицензированного ПО | Приобретение и установка лицензированного ПО |
|  | Доверенности | Несанкционированное копирование бумажных носителей | 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 |
| Кража бумажных носителей | 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 |
| Уничтожение бумажных носителей (пожар) | 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 и пожарной сигнализации для помещения/ установка средств пожаротушения |
|  | Распоряжения и поручения | Несанкционированное копирование, удаление, модификация данных на сервере | Доступ в помещение по ID-карте/ установка системы видеонаблюдения/установка системы охранной сигнализации/аутентификация по SSH для доступа к серверу/ периодическое создание бэкапа/аудит файлов с помощью IDS/IPC/запрет использования сотрудниками внешних носителей/использование антивирусного ПО и файрвола/использование программного средства защиты информации от НСД. |
| Чтение или фотографирование информации с экранов ПК компьютеров сотрудников | Использование защитной пленки на стеклах окон/проведение обучающего инструктажа по ИБ/ использование системы Screen Guard |
| Несанкционированное распечатывание электронной версии документа | Печать с автоматической маркировкой каждой страницы и автоматическим оформлением учётной карточки документа с указанием даты печати, учётных реквизитов, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности, фамилии лица, выдавшего документ, количества страниц и копий документа. |
| Физическое воздействие на сервер | 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 |
| Заражение вредоносным ПО | Использование антивирусного ПО/ установка файрвола/ запрет использования сотрудниками внешних носителей, не предусмотренных первоначальной комплектацией / периодическое создание бэкапа архива документов/ установка системы видеонаблюдения |
| Использование нелицензированного ПО | Приобретение и установка лицензированного ПО |
| Разглашение данных сотрудниками организации | Инструктаж сотрудников по ИБ/ обеспечение конфиденциальности данных путем заключения соглашения о неразглашении конфиденциальных данных сотрудниками |
|  | Кадровая информация | Несанкционированное копирование, удаление, модификация данных на сервере | Доступ в помещение по ID-карте/ установка системы видеонаблюдения/установка системы охранной сигнализации/аутентификация по SSH для доступа к серверу/ периодическое создание бэкапа/аудит файлов с помощью IDS/IPC/запрет использования сотрудниками внешних носителей/использование антивирусного ПО и файрвола/использование программного средства защиты информации от НСД. |
| Чтение или фотографирование информации с экранов ПК компьютеров сотрудников | Использование защитной пленки на стеклах окон/проведение обучающего инструктажа по ИБ/ использование системы Screen Guard |
| Несанкционированное распечатывание электронной версии документа | Печать с автоматической маркировкой каждой страницы и автоматическим оформлением учётной карточки документа с указанием даты печати, учётных реквизитов, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности, фамилии лица, выдавшего документ, количества страниц и копий документа. |
| Несанкционированное копирование бумажных носителей | 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 |
| Кража бумажных носителей | 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 |
| Уничтожение бумажных носителей (пожар) | 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 |
| Разглашение данных сотрудниками организации | Инструктаж сотрудников по ИБ/ обеспечение конфиденциальности данных путем заключения соглашения о неразглашении конфиденциальных данных сотрудниками |
| Физическое воздействие на сервер | 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 |
| Заражение вредоносным ПО | Использование антивирусного ПО/ установка файрвола/ запрет использования сотрудниками внешних носителей, не предусмотренных первоначальной комплектацией / периодическое создание бэкапа архива документов/ установка системы видеонаблюдения |
| Использование нелицензированного ПО | Приобретение и установка лицензированного ПО |
|  | Сведения о лицензии | Физическое воздействие на сервер | 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 |
| Несанкционированное копирование, удаление, модификация данных на сервере | Доступ в помещение по ID-карте/ установка системы видеонаблюдения/установка системы охранной сигнализации/аутентификация по SSH для доступа к серверу/ периодическое создание бэкапа/аудит файлов с помощью IDS/IPC/запрет использования сотрудниками внешних носителей/использование антивирусного ПО и файрвола/использование программного средства защиты информации от НСД |
| Заражение вредоносным ПО | Использование антивирусного ПО/ установка файрвола/ запрет использования сотрудниками внешних носителей, не предусмотренных первоначальной комплектацией / периодическое создание бэкапа архива документов/ установка системы видеонаблюдения |

Выводы:

В результате выполнения лабораторной работы был проведен анализ информационных ресурсов нотариальной конторы. На основании полученных результатов были выделены информационные активны организации, к которым относятся: учетно – отчетная документация (включает в себя книги специального учета, реестры), персональные данные сотрудников, персональные данные клиентов, номенклатурные дела, сведения о техническом состоянии ЭВМ, информация о заключенных нотариальных сделках, необходимая для регистрации в книгах специального учета и реестрах, доверенности, позволяющие помощникам заключать сделки, проводить консультации от имени нотариуса, распоряжения и поручения.

Выявленные информационные активы были классифицированы по степени значимости обеспечения конфиденциальности, целостности и доступности, а также соотнесены к категориям видов тайн.

Тщательный анализ структуры и деятельности организации позволил выявить наиболее опасные и вероятные каналы утечки информации. Но основании полученных данных были разработаны средства и способы противодействия несанкционированному распространению информации.

Список литературы:

* + - 1. Классификация информационных активов, URL: <https://ipiskunov.blogspot.com/2016/07/blog-post_0.html>
      2. Основные каналы утечки инормации, URL: <https://rt-solar.ru/products/solar_dozor/blog/2085/>
      3. Утечка информации, URL: <https://irsural.ru/poleznaya-informaciya/utechka-informacii/>
      4. Информационная система нотариуса «еНот», URL: <https://www.triasoft.com/programs3.htm>
      5. Screen Guard, URL: <https://secretgroup.ru/screen-guard/>