### **Инструкция к выполнению домашнего задания**

1. Сделайте копию шаблона себе на Google Disk.
2. Выполните домашнее задание в шаблоне.
3. Для проверки домашнего задания отправьте ссылку на ваш документ в личном кабинете Нетологии.
4. Перед тем как выслать ссылку, убедитесь, что ее содержимое не является приватным (открыто на просмотр всем, у кого есть ссылка). Если необходимо прикрепить дополнительные ссылки, просто добавьте их в свой Google Docs.
5. Любые вопросы по решению задач задавайте в чате учебной группы.

**Ответ к заданию. Моделирование угроз**

**Вопрос 1.**

Напишите возможные негативные последствия от реализации (возникновения) угроз безопасности информации. 3 самых негативных для выбранного актива. Напишите, почему выбрали их.

Актив предприятия для которого разрабатывается модель угроз:

***ИСПДн – электроггая БД отдела кадров организации «Новейшие технологии»***

**!!!В работе используйте Приложение 4** из [Методики оценки угроз безопасности от ФСТЭК России от 05 февраля 2021 г.](https://u.netology.ru/backend/uploads/lms/attachments/files/data/54611/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82_%D0%BE%D1%82_5_%D1%84%D0%B5%D0%B2%D1%80%D0%B0%D0%BB%D1%8F_2021_%D0%B3.__1_.pdf)

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Виды риска** | **Негативные последствия** | **Обоснование** |
| 1 | Ущерб физическому лицу | Нарушение конфиденциальности (утечка) персональных данных. | Сведения о физическом лице могут стать известны третьим лицам, могут быть проданы и использоваться в мошеннических схемах или для шантажа |
| 2 | Ущерб физическому лицу | Разглашение персональных данных граждан | Разглашение ПДн также негативно влияет на физические лица, и может использоваться в мошеннических схемах и вымогательстве. |
| 3 | Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью | Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса.  Нарушение деловой репутации.  Снижение престижа. | Негативное влияние на систему обработки ПДн, что может привести к ее остановке на время расследования инцидента утечки данных, либо восстановления если система была повреждена в результате атаки. |

**Вопрос 2**.

Какие есть возможные объекты воздействия угроз безопасности информации? Напишите не менее 3-х.

**!!!В работе используйте Приложение 5** из [Методики оценки угроз безопасности от ФСТЭК России от 05 февраля 2021 г.](https://u.netology.ru/backend/uploads/lms/attachments/files/data/54611/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82_%D0%BE%D1%82_5_%D1%84%D0%B5%D0%B2%D1%80%D0%B0%D0%BB%D1%8F_2021_%D0%B3.__1_.pdf)

|  |  |
| --- | --- |
| **№** | **Возможные объекты воздействия угроз безопасности** |
| 1 | База данных информационной системы, содержащая персональные данные работников |
| 2 | АРМ сотрудников, работающих с системой обработки ПДн |
| 3 | Локальная вычислительная сеть, соединяющая АРМ сотрудников и сервер БД с ПДн сотрудников организации |

**Вопрос 3**.

Опишите возможные способы реализации (возникновения) угроз безопасности информации. Напишите не менее 5-ти.

**!!!В работе используйте Приложение 10** из [Методики оценки угроз безопасности от ФСТЭК России от 05 февраля 2021 г.](https://u.netology.ru/backend/uploads/lms/attachments/files/data/54611/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82_%D0%BE%D1%82_5_%D1%84%D0%B5%D0%B2%D1%80%D0%B0%D0%BB%D1%8F_2021_%D0%B3.__1_.pdf)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Вид нарушителя** | **Категория нарушителя** | **Объект воздействия** | **Доступные интерфейсы** | **Способы реализации** |
| 1 | Авторизованные пользователи систем и сетей | Внутренний | Электронная база данных, содержащая персональные данные сотрудников предприятия | Доступ через локальную вычислительную сеть организации | Неправильно настроенные администратором безопасности СЗИ (дискреционные, мандатные права доступа) |
| 2 | Системные администраторы и администраторы безопасности | Внутренний | Электронная база данных, содержащая персональные данные сотрудников предприятия | Доступ через локальную вычислительную сеть организации | Использование учетных записей, обладающих привилегированными правами |
| 3 | Системные / сетевые администраторы | Внутренний | Локальная вычислительная сеть, соединяющая АРМ сотрудников и сервер БД с ПДн сотрудников организации | Доступ через локальную вычислительную сеть организации | Неправильная или ошибочная настройка МЭ или роутера, позволяющая злоумышленнику получить доступ к оборудованию из вне. |
| 4 | Отдельные физические лица (хакеры) | Внешний | Электронная база данных, содержащая персональные данные сотрудников предприятия - несанкционированный доступ к информации | Доступ через локальную вычислительную сеть организации | Внедрение вредоносного программного обеспечения |
| 5 | Отдельные физические лица (хакеры) | Внешний | АРМ сотрудников, работающих с системой обработки ПДн | Доступ через локальную вычислительную сеть организации | Внедрение троянов и эксплойтов на АРМ сотрудника, работающего с БД ИСПДн с целью кражи пароля доступа к системе обработки ПДн |