Правительство Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Курсовая работа

по дисциплине

«Основы информационной безопасности»

Работу выполнил

Студент группы СКБ221 Т. Б. Смирнов

Содержание

Введение

В домашней работе в качестве объекта информатизации будет рассмотрена Автошкола “Возьми и сдай”, включающая в себя следующие внутренние отделы:

- Бухгалтерия

Составляет бухгалтерские отчеты, связанные с автомобилями и учениками.

- Отдел по работе с учениками (Администратор)

Общается с клиентами. Узнает о существующих проблемах, подбирает соответствующие курсы и цену. При необходимости дает консультации по поводу существующих проблем, предоставляет поддержку ученикам, собирает контактную информацию. Вся информация передается в бухгалтерию. Осуществляет связь между учеником и ГИБДД.

- Инструктор

Проводит занятия с учениками, договаривается о датах встреч и рассматривает личные пожелания об обучении клиентов.

- Автопарк

Следит за состоянием автомобилей, отправляет их на плановое техническое обслуживание и ремонт в случае поломок в автомобильный сервис. Отправляет счета в бухгалтерию.

Объект информатизации

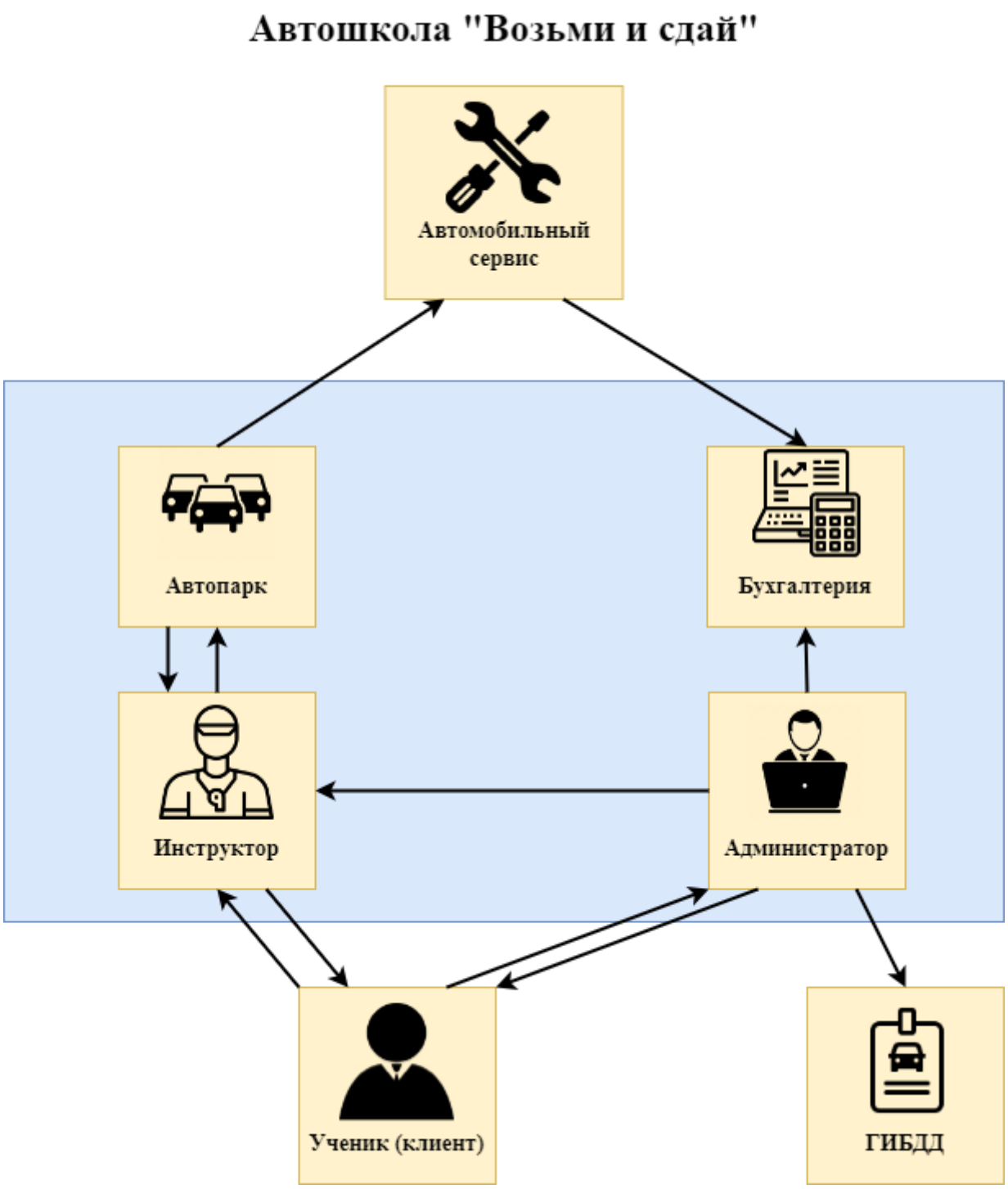


Рисунок 1. Объект информатизации

Способы передачи данных

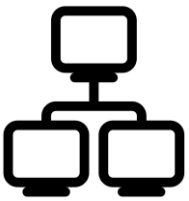
Локальная сеть	
Мобильная связь	
Речь	
Письмо по почте	

Таблица 1. Обозначения способов передачи данных

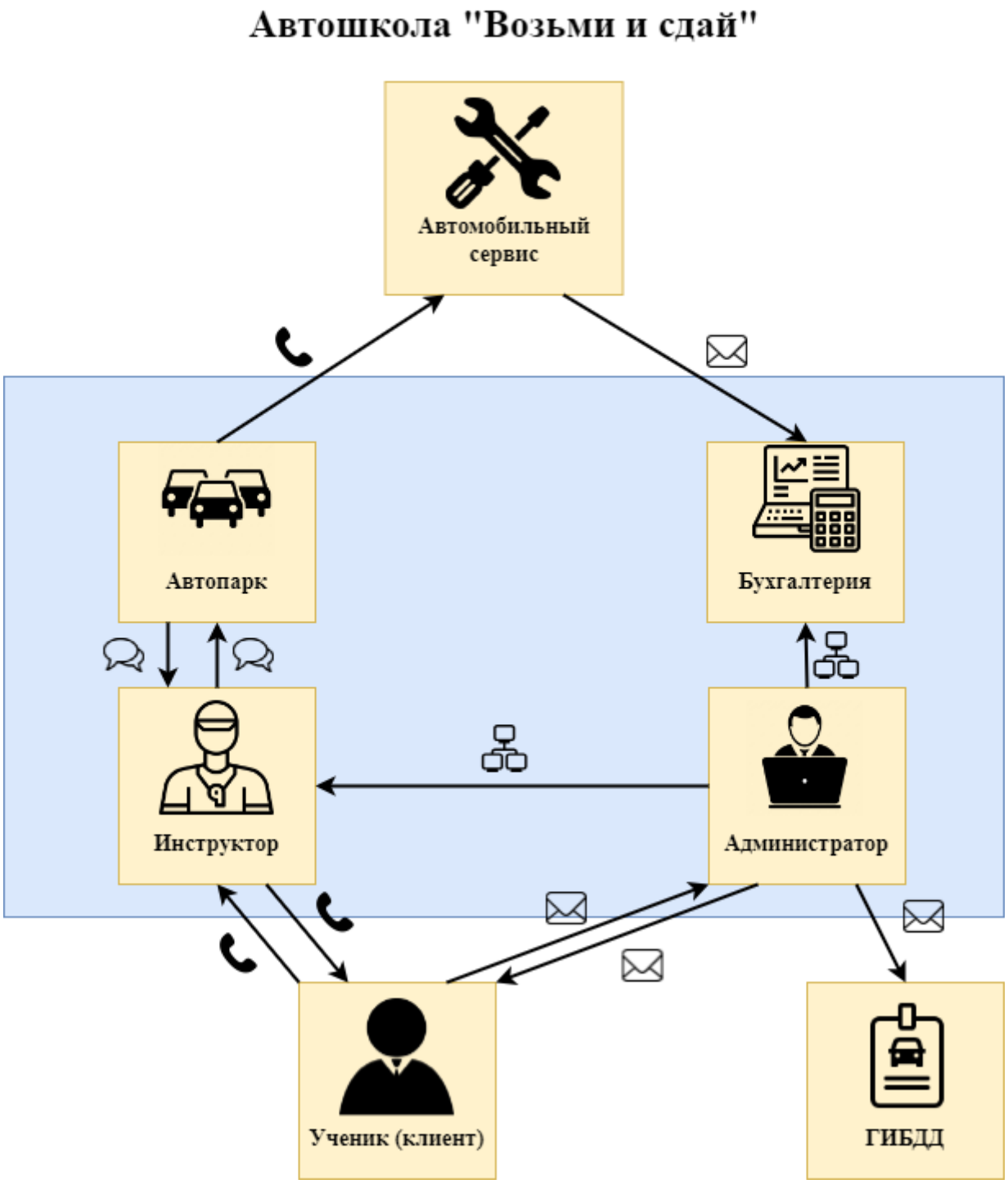


Рисунок 2. Способы передачи данных

Определение свойств информации, которые необходимо обеспечить

№	Взаимо-действие	Способ передачи информа-ции	Назначение информац-ионных потоков	Свойства информации, которые необходимо обеспечить	Пояснение
1	Администратор => ГИБДД	Письмо по почте	Передача информации об учениках для записи на экзамен	1. Конфиденциальность Обеспечение приватности персональных данных учеников. 2. Целостность Неизменность передаваемых данных о каждом ученике. 3. Доступность Беспрепятственная реализация права доступа ГИБДД на информацию об учениках.	
2	Администратор => Ученик	Письмо по почте	Передача информации об обучении	1. Целостность Неизменность передаваемых данных об обучении в автошколе. 2. Доступность Беспрепятственная реализация права доступа учеников на информацию об обучении.	Конфиденци-альность можно не обеспечивать так как данная информация общедостп-ная

3	Администратор => Инструктор	Локальная сеть	Передача информации об учениках	1. Конфиденциальность Обеспечение приватности персональных данных учеников. 2. Целостность Неизменность передаваемых данных о каждом ученике. 3. Доступность Беспрепятственная реализация права доступа инструктора на информацию об учениках.	
4	Администратор => Бухгалтерия	Локальная сеть	Передача информации об учениках	1. Целостность Неизменность передаваемых данных о каждом ученике. 2. Доступность Беспрепятственная реализация права доступа бухгалтерии на информацию об учениках.	Конфиденциальность можно не обеспечивать так как данная информация общедостпная
5	Ученик => Администратор	Письмо по почте	Передача персональных данных	1. Конфиденциальность Обеспечение приватности персональных данных учеников.	Доступность обеспечивает не отдел информационной безопасности объекта информатизации

6	Ученик => Инструктор	Мобильная связь	Передача информации о свободном времени	1. Конфиденциальность Обеспечение приватности персональных данных учеников.	Доступность и целостность обеспечивает не отдел информационной безопасности объекта информатизации
7	Инструктор => Ученик	Мобильная связь	Передача информации о занятиях	1. Целостность Неизменность передаваемых данных.	Конфиденциальность можно не обеспечивать так как данная информация общедостпная. Доступность обеспечивает не отдел информационной безопасности объекта информатизации.
8	Инструктор => Автопарк	Речь	Передача информации о нужном автомобиле	1. Целостность Неизменность передаваемых данных.	Конфиденциальность можно не обеспечивать так как данная информация не является приватной. Доступность обеспечивает не отдел

					информационной безопасности объекта информатизации.
9	Автопарк => Инструктор	Речь	Передача информации о свободных автомобилях	1. Целостность Неизменность передаваемых данных.	Конфиденциальность можно не обеспечивать так как данная информация не является приватной. Доступность не отделом.
10	Автопарк => Автомобильный сервис	Мобильная связь	Передача информации о состояниях автомобилей	1. Целостность Неизменность передаваемых данных. 2. Доступность Беспрепятственная реализация права доступа сервиса на информацию об автомобилях.	Конфиденциальность можно не обеспечивать так как данная информация не является приватной.
11	Автомобильный сервис => Бухгалтерия	Письмо по почте	Передача информации о стоимости работ	1. Конфиденциальность Обеспечение приватности персональных данных учеников.	Доступность и целостность обеспечивает не отдел информационной безопасности объекта информатизации.

Таблица 2. Информационные потоки

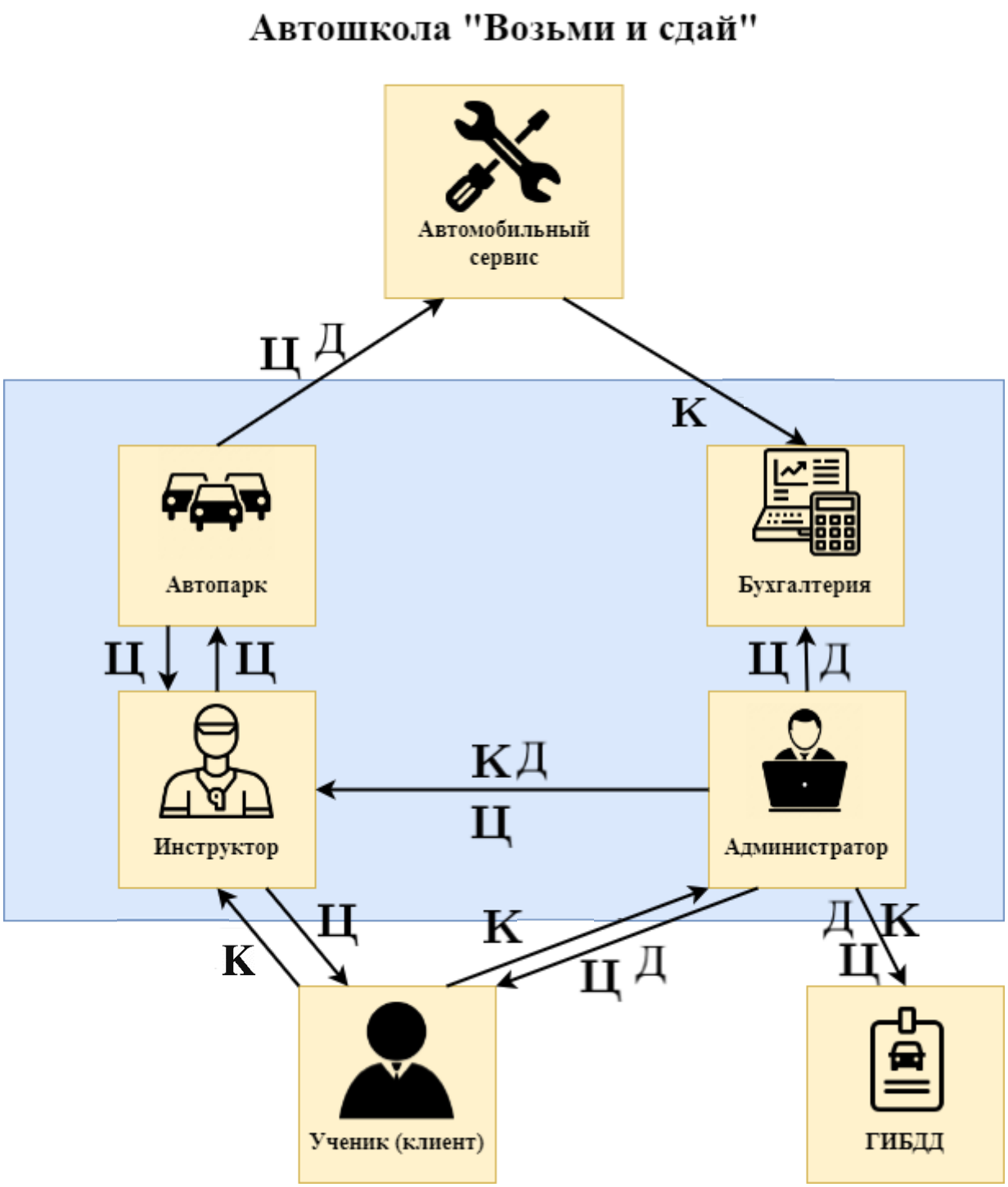


Рисунок 3. Свойства передаваемой информации

Определение возможных негативных последствий от реализации угроз безопасность информации

№	Виды риска (ущерба)	Возможные негативные последствия
У1	Ущерб физическому лицу (в данном случае ученикам)	Нарушение тайны переписки, телефонных переговоров, иных сообщений. Финансовый, иной материальный ущерб физическому лицу. Разглашение персональных данных.

У2	Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью	Потеря (хищение) денежных средств. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. Необходимость дополнительных затрат на закупку товаров, работ или услуг (в том числе закупка ПО, технических средств, вышедших из строя, замена, настройка, ремонт, указанных средств). Срыв запланированной сделки с партнером. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Потеря клиентов. Потеря конкурентного преимущества. Невозможность заключения договоров, соглашений. Нарушение деловой репутации. Снижение престижа. Утрата доверия. Причинение имущественного ущерба. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)

Таблица 3. Виды рисков (ущерба) и типовые негативные последствия от реализации угроз безопасности информации

Определение объектов воздействия и видов воздействия на них

№	Негативные последствия	Объекты воздействия	Виды воздействия
У1	Нарушение тайны переписки, телефонных переговоров, иных сообщений.	Электронный почтовый ящик администратора.	Утечка идентификационной информации граждан.
	Финансовый, иной материальный ущерб физическому лицу.	Удаленное автоматизированное место (АРМ) работника отдела по работе с учениками.	Утечка реквизитов платежных поручений граждан с АРМ работника отдела по работе с учениками.
	Нарушение конфиденциальности(утечка) персональных данных.	Удаленное автоматизированное место (АРМ) оператора отдела по работе с клиентами.	Утечка идентификационной информации и персональных данных граждан с АРМ работника отдела по работе с учениками.

	Разглашение персональных данных.	Удаленное автоматизированное место (АРМ) оператора отдела по работе с клиентами. .	Утечка идентификационной информации и персональных данных граждан с АРМ работника отдела по работе с учениками.
У2	Потеря (хищение) денежных средств.	АРМ финансового директора (бухгалтерия).	Несанкционированная модификация информации в платежных распоряжениях и отправка недостоверных распоряжений от имени финансового директора.
		Электронный почтовый ящик финансового директора.	Модификация информации в платежных распоряжениях и отправка недостоверных распоряжений от имени финансового директора.
		АРМ главного бухгалтера.	Подмена данных, содержащих реквизиты платежных поручений и другой платежной информации на АРМ главного бухгалтера.

	Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций.	Удаленное автоматизированное место (АРМ) работника отдела по работе с учениками.	Утечка реквизитов платежных поручений граждан с АРМ оператора.
	Необходимость дополнительных затрат на закупку товаров, работ или услуг (в том числе закупка ПО, технических средств, вышедших из строя, замена, настройка, ремонт, указанных средств).	Линия связи между автоинструктором и автомобильным парком.	Подмена данных, содержащих информацию о нужном автомобиле и времени его выдачи.
	Срыв запланированной сделки с партнером.	АРМ работника отдела по работе с учениками.	Модификация информации и отправка данных с недостоверной информацией от имени работника отдела по работе с учениками.
		Электронный почтовый ящик работника отдела по работе с учениками.	Модификация информации и отправка электронных писем с недостоверной информацией от имени работника отдела по работе с учениками.
	Необходимость дополнительных (незапланированных) затрат на восстановление деятельности.	АРМ сотрудника автомобильного парка.	Несанкционированная модификация информации по состоянию и ремонту автомобилей.

	Потеря клиентов.	АРМ администратора.	Отказ в обслуживании сайта и других систем связи. Внедрение вредоносного ПО с целью нарушения работы сайта и других систем связи.
	Потеря конкурентного преимущества.	АРМ сотрудника автомобильного парка.	Утечка приватной информации о сотрудничестве с определенным автомобильным сервисом.
	Невозможность заключения договоров, соглашений.	АРМ администратора.	Отказ в обслуживании сайта и других систем связи. Внедрение вредоносного ПО с целью нарушения работы сайта и других систем связи.
	Нарушение деловой репутации.	АРМ администратора.	Отказ в обслуживании сайта и других систем связи. Внедрение вредоносного ПО с целью нарушения работы сайта и других систем связи.
		АРМ сотрудника автомобильного парка.	Утечка приватной информации о сотрудничестве с определенным автомобильным сервисом.
	Снижение престижа.	АРМ работника отдела по работе с учениками.	Модификация информации и отправка данных с недостоверной информацией от имени работника отдела по

			работе с учениками. Публикация Провокационных материалов на сайте компании и личных страницах в социальных сетях от имени работника отдела по работе с учениками.
	Утрата доверия.	АРМ администратора.	Утечка идентификационной информации и персональных данных граждан с АРМ оператора.
		АРМ сотрудника автомобильного парка.	Утечка приватной информации о сотрудничестве с определенным автомобильным сервисом.
	Причинение имущественного ущерба.	АРМ сотрудника компании.	Механическое повреждение.
	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).	АРМ сотрудника автомобильного парка.	Несанкционированная модификация информации по состоянию и ремонту автомобилей.
	Утечка конфиденциальной информации	АРМ сотрудника компании.	Внедрение вредоносного ПО с целью получения

	(коммерческой тайны, секретов производства (ноу-хау) и др.)		конфиденциальных данных.

Таблица 4. Определение объектов воздействия и видов воздействия на них

Определение источников угроз безопасности информации

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	У1	У2	У3	
Специальные службы иностранных государств	-	-	-	-
Террористические, экстремистские группировки	-	-	-	-
Преступные группы (криминальные структуры)	+ (получение финансовой выгоды за счет кражи и продажи персональных данных граждан)	+ (Получение финансовой выгоды за счет кражи и коммерческой тайны. Желание самореализации)	-	У1 (Финансовый, иной материальный ущерб физическому лицу. Нарушение конфиденциальности(утечка) персональных данных.) У2 (Потеря (хищение) денежных средств. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций.

				Необходимость дополнительных затрат на закупку товаров, работ или услуг (в том числе закупка ПО, технических средств, вышедших из строя, замена, настройка, ремонт, указанных средств). Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Нарушение деловой репутации. Причинение имущественного ущерба. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.))
Отдельные физические лица (хакеры)	+ (получение финансовой выгоды за счет кражи и продажи персональных данных граждан)	+ (получение финансовой выгоды за счет кражи и коммерческой тайны. желание самореализации)	-	У1 (Нарушение тайны переписки, телефонных переговоров, иных сообщений. Финансовый, иной материальный ущерб физическому лицу. Нарушение конфиденциальности(утечка) персональных данных.) У2

				(Потеря (хищение) денежных средств. Срыв запланированной сделки с партнером. Причинение имущественного ущерба. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.))
Конкурирующие организации	-	+ (Получение конкурентных преимуществ. получение финансовой выгоды за счет кражи и коммерческой тайны)	-	У2 (Потеря (хищение) денежных средств. Срыв запланированной сделки с партнером. Потеря клиентов. Потеря конкурентного преимущества. Невозможность заключения договоров, соглашений. Нарушение деловой репутации. Снижение престижа. Утрата доверия. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.))

Разработчики программных, программно-аппаратных средств	-	+ (Получение конкурентных преимуществ. получение финансовой выгоды за счет кражи и коммерческой тайны)	-	У2 (Потеря конкурентного преимущества. Причинение имущественного ущерба. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.))
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	-	+ (получение финансовой выгоды за счет кражи и коммерческой тайны. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ.)	-	У2 (Потеря (хищение) денежных средств. Потеря клиентов. Потеря конкурентного преимущества. Причинение имущественного ущерба. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)))

Поставщики вычислительных услуг, услуг связи	-	+ (получение финансовой выгоды за счет кражи и коммерческой тайны. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ)	-	У2 (Потеря (хищение) денежных средств. Потеря клиентов. Потеря конкурентного преимущества.Причинение имущественного ущерба. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций))
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	-	+ (получение финансовой выгоды за счет кражи и коммерческой тайны Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ)	-	У2 (Необходимость дополнительных затрат на закупку товаров, работ или услуг (в том числе закупка ПО, технических средств, вышедших из строя, замена, настройка, ремонт, указанных средств). Потеря конкурентного преимущества. Причинение имущественного ущерба. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).

				Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.))
Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	-	+ (получение финансовой выгоды за счет кражи и коммерческой тайны. Непреднамеренные, неосторожные или неквалифицированные действия)	-	У2 (Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Причинение имущественного ущерба. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.))

Авторизованные пользователи систем и сетей	-	+ (получение финансовой выгоды за счет кражи и коммерческой тайны. Любопытство или желание самореализации. Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия)	-	У2 (Потеря (хищение) денежных средств. Необходимость дополнительных затрат на закупку товаров, работ или услуг (в том числе закупка ПО, технических средств, вышедших из строя, замена, настройка, ремонт, указанных средств).Срыв запланированной сделки с партнером. Причинение имущественного ущерба. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.))
Системные администраторы и администраторы безопасности	+ (Месть за ранее совершенные действия.)	+ (получение финансовой выгоды за счет кражи и коммерческой тайны. Любопытство или желание самореализации. Месть за ранее совершенные действия.	-	У1 (Разглашение персональных данных.) У2 (Потеря (хищение) денежных средств. Срыв запланированной сделки с партнером. Потеря клиентов. Потеря конкурентного преимущества. Нарушение деловой репутации. Утрата доверия.

		Непреднамеренные, неосторожные или неквалифицированные действия.)		Причинение имущественного ущерба.)
Бывшие работники (пользователи)	+ (Месть за ранее совершенные действия.)	+ (получение финансовой выгоды за счет кражи и коммерческой тайны. Месть за ранее совершенные действия.)	-	У1 (Нарушение тайны переписки, телефонных переговоров, иных сообщений. Разглашение персональных данных.) У2 (Нарушение деловой репутации. Необходимость дополнительных затрат на закупку товаров, работ или услуг (в том числе закупка ПО, технических средств, вышедших из строя, замена, настройка, ремонт, указанных средств). Снижение престижа. Утрата доверия. Причинение имущественного ущерба.)

Таблица 5. Оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации

Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
У1 (Нарушение тайны переписки, телефонных переговоров, иных сообщений. Финансовый, иной материальный ущерб физическому лицу. Нарушение конфиденциальности(утечка) персональных данных. Разглашение персональных данных.	Отдельные физические лица (хакеры)	Внешний	Н1
	Бывшие работники (пользователи)	Внешний	Н1
	Преступные группы (криминальные структуры)	Внешний	Н2
	Системные администраторы и администраторы безопасности	Внутренний	Н2
	Конкурирующие организации	Внешний	Н2
	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1
	Поставщики вычислительных услуг, услуг связи	Внутренний	Н2
	Авторизованные пользователи систем и сетей	Внутренний	Н1

У2 (Потеря (хищение) денежных средств. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. Необходимость дополнительных затрат на закупку товаров, работ или услуг (в том числе закупка ПО, технических средств, вышедших из строя, замена, настройка, ремонт, указанных средств). Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Нарушение деловой репутации. Причинение имущественного ущерба. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) Срыв запланированной сделки с партнером. Потеря клиентов. Потеря конкурентного преимущества.	Системные администраторы и администраторы безопасности	Внутренний	H2
	Преступные группы (криминальные структуры)	Внешний	H2
	Отдельные физические лица (хакеры)	Внешний	H1
	Конкурирующие организации	Внешний	H2
	Разработчики программных, программно-аппаратных средств	Внутренний	H3
	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	H1
	Поставщики вычислительных услуг, услуг связи	Внутренний	H2
	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных	Внутренний	H2

Невозможность заключения договоров, соглашений. Снижение престижа. Утрата доверия. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций))	и иных видов работ		
	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Внутренний	H1
	Авторизованные пользователи систем и сетей	Внутренний	H1
	Бывшие работники (пользователи)	Внешний	H1

Таблица 6. Актуальные нарушители при реализации угроз безопасности информации и соответствующие им возможности

Определение способов реализации (возникновения) угроз безопасности информации

№	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
1	Преступные группы (криминальные структуры) (H2)	внешний	Удаленное автоматизированное место (АРМ) работника отдела по работе с учениками.	Доступ через LAN-сеть организации	Внедрение вредоносного ПО (программного обеспечения)
			АРМ финансового директора (бухгалтерия).		
2	Отдельные физические лица (хакеры) (H1)	внешний	Удаленное автоматизированное место (АРМ) работника отдела по работе с учениками.	Рассылка писем с фишингом	Кража персональных данных сотрудника, ввиду его непрофессионализма и внедрение вредоносного ПО и получение удаленного доступа к АРМ сотрудника
			Электронный почтовый ящик финансовог		

			о директора.		
3	Конкурирующие организации (Н2)	внешний	(АРМ) работника отдела по работе с учениками.	Доступ через LAN-сеть организации	Внедрение вредоносного ПО
			АРМ сотрудника автомобильного парка.		
			Электронный почтовый ящик финансового директора.	Рассылка фишинговых писем	Кража персональных данных сотрудника и владеемой им информацией.
			Электронный почтовый ящик администратора.		
4	Разработчики программных, программно-аппаратных средств (Н3)	внутренний	Удаленное автоматизированное место (АРМ) работника отдела по работе с учениками.	Доступ через LAN-сеть организации	Внедрение вредоносного ПО

			АРМ сотрудника автомобильного парка.	Съемные машинные носители информации, подключаемые к АРМ сотрудника	Использование уязвимостей конфигурации системы программного обеспечения
			АРМ финансового директора (бухгалтерия).		
5	Поставщики вычислительных услуг, услуг связи (Н2)	внешний	Удаленное автоматизированное место (АРМ) работника отдела по работе с учениками.	Неосторожность или непрофессионализм данных лиц	Механические повреждения.
				Съемные машинные носители информации, подключаемые к АРМ сотрудника	Использование уязвимостей конфигурации АРМ сотрудника
6	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных	внутренний	АРМ главного бухгалтера.	Съемные машинные носители информации, подключаемые к АРМ сотрудника	Внедрение вредоносного ПО
					Использование уязвимостей конфигурации АРМ сотрудника
			АРМ сотрудника автомобильного парка.	Неосторожность или непрофессионализм данных лиц	Механические повреждения.

	видов работ (Н2)		АРМ работника отдела по работе с учениками.		
7	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем (Н2)	внешний	АРМ работника автопарка.	Поставка программных, программно-аппаратных средств, обеспечивающих систем с уязвимостями в коде	Использование уязвимостей кода ПО
8	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администт	внутренний	АРМ работника отдела по работе с учениками.	Неосторожность или непрофессионализм данных лиц при работе с соответствующим инвентарем	Механические повреждения.
			АРМ главного бухгалтера.	Съемные машинные носители информации, подключаемые	Дублирование приватной информации на съемные

	рация, охрана, уборщики и т.д.) (Н1)		АРМ сотрудника автомобильного парка.	к АРМ сотрудника	машинные носители информации
9	Системные администраторы и администраторы безопасности (Н2)	внутренний	АРМ главного бухгалтера.	Съемные машинные носители информации, подключаемые к АРМ сотрудника	Дублирование приватной информации на съемные машинные носители информации
10	Авторизованные пользователи систем и сетей (Н1)	внутренний	АРМ работника отдела по работе с учениками.	Неосторожность или непрофессионализм данных лиц	Механические повреждения
				Съемные машинные носители информации, подключаемые к АРМ сотрудника	Дублирование приватной информации на съемные машинные носители информации
11	Бывшие работники (пользователи) (Н1)	внешний	Электронный почтовый ящик администратора.	Рассылка фишинговых писем	Кража персональных данных сотрудника и владеемой им информацией.

				Умышленное нанесение ущерба подручными средствами	Механические повреждения

Таблица 7. Актуальные способы реализации угроз безопасности информации и соответствующие им виды нарушителей и возможности

Определение угроз безопасности информации

$УБИ_1$ = [Другая автошкола, находящаяся неподалеку (Конкурирующие организации); АРМ работника бухгалтерии; внедрение вредоносного ПО; Потеря конкурентного преимущества и Срыв запланированной сделки с партнером]

$УБИ_2$ = [Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ; АРМ работника автопарка; использование уязвимостей конфигурации; Необходимость дополнительных затрат на закупку товаров, работ или услуг (в том числе закупка ПО, технических средств, вышедших из строя, замена, настройка, ремонт, указанных средств) и Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)]

$УБИ_3$ = [Хакерская организация “ШаМаН”(Преступные группы (криминальные структуры)); АРМ администратора; внедрение вредоносного ПО; Нарушение деловой репутации и Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)]

$УБИ_4$ = [Разработчики программных, программно-аппаратных средств; АРМ работника отдела по работе с учениками; Использование уязвимостей конфигурации системы программного обеспечения; Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) и Потеря конкурентного преимущества.]

$УБИ_5$ = [Уборщица, недавно начала работу в организации (Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)); Линия связи между администратором и бухгалтерией; Повреждение LAN-кабеля (Механические повреждения); Необходимость дополнительных (незапланированных) затрат на восстановление деятельности и Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).]

$УБИ_6$ = [хакер Ivan (Отдельные физические лица (хакеры)); Электронный почтовый ящик администратора; Кража персональных данных сотрудника; Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) и Срыв запланированной сделки с партнером]

$УБИ_7$ = [Сотрудник другой автошколы, находящейся неподалеку (Конкурирующие организации); АРМ администратора; внедрение вредоносного ПО; Срыв запланированной сделки с партнером, Потеря клиентов, Потеря конкурентного преимущества и Утрата доверия]

$УБИ_8$ = [Поставщики вычислительных услуг, услуг связи; АРМ работника автопарка; Повреждение устройства связи (Механические повреждения); Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)]

$УБИ_9$ = [Лица, обеспечивающие поставку программных, программно- аппаратных средств, обеспечивающих систем; Линия связи между инструктором и автопарком; Использование генераторов радиоэлектронных волновых генераторов для нарушения целостности передаваемой информации; Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)]

$УБИ_{10}$ = [Бывшие работники (пользователи); телефон инструктора для связи с учениками; Умышленное повреждение устройства (Механические повреждения); Нарушение деловой репутации и Необходимость дополнительных затрат на закупку товаров, работ или услуг (в том числе закупка ПО, технических средств, вышедших из строя, замена, настройка, ремонт, указанных средств)]

$УБИ_{11}$ = [Инструктор из другой автошколы (Отдельные физические лица (хакеры)); Основное устройство работы инструктора, связи с учениками; Внедрение вредоносного ПО, использование

уязвимостей; Срыв запланированной сделки с партнером и Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)]

Определение перечня актуальных угроз безопасности информации

$УБИ_1$ = [Другая автошкола, находящаяся неподалеку (Конкурирующие организации); АРМ работника бухгалтерии; внедрение вредоносного ПО; Потеря конкурентного преимущества и Срыв запланированной сделки с партнером]

Сценарий реализации:

- T1 - Сбор информации о системах и сетях:
  - T1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
  - T1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях - идентификационной информации пользователей
  - T1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга
- T2 - Получение первоначального доступа к компонентам систем и сетей:
  - T2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет)
  - T2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке
  - T2.4. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке

- Т2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы

- Т6 - Повышение привилегий по доступу к компонентам систем и сетей:
  - Т6.2. Подбор пароля или другой информации для аутентификации от имени привилегированной учетной записи
- Т7 - Сокрытие действий и применяемых при этом средств от обнаружения:
  - Т7.1. Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения.
  - Т7.2. Очистка/затирание истории команд и журналов регистрации, перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей
- Т10 - Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:
  - Т10.7. Подмена информации (например, платежных реквизитов) в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей

Указанные тактики и техники доступны для данного нарушителя.

⇨ $УБИ_1$ актуальна

$УБИ_2$ = [Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ; АРМ работника автопарка; использование уязвимостей конфигурации; Необходимость дополнительных затрат на закупку товаров, работ или услуг (в том числе закупка ПО, технических средств, вышедших из строя, замена, настройка, ремонт, указанных средств) и Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)]

Сценарий реализации:

- Т1 - Сбор информации о системах и сетях:
  - Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
  - Т1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях - идентификационной информации пользователей
- Т3 - Внедрение и исполнение вредоносного программного обеспечения в системах и сетях:
  - Т3.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии
- Т7 - Сокрытие действий и применяемых при этом средств от обнаружения:
  - Т7.10. Внедрение вредоносного кода в доверенные процессы операционной системы и другие объекты, которые не подвергаются анализу на наличие такого кода, для предотвращения обнаружения
- Т10 - Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:

- Т10.2. Несанкционированное воздействие на системное программное обеспечение, его конфигурацию и параметры доступа

Указанные тактики и техники доступны для данного нарушителя.

⇨ $УБИ_2$ актуальна

$УБИ_3$ = [Хакерская организация “ШаМаН”(Преступные группы (криминальные структуры)); АРМ администратора; внедрение вредоносного ПО; Нарушение деловой репутации и Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)]

Сценарий реализации:

- Т1 - Сбор информации о системах и сетях:
  - Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
  - Т1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях - идентификационной информации пользователей
- Т2 - Получение первоначального доступа к компонентам систем и сетей:
  - Т2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет)
  - Т2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы
- Т3 - Внедрение и исполнение вредоносного программного обеспечения в системах и сетях:
  - Т3.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских

или системных учетных данных, в том числе с использованием методов социальной инженерии

- Т7 - Сокрытие действий и применяемых при этом средств от обнаружения:
  - Т7.1. Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения.
  - Т7.3. Удаление файлов, переписывание файлов произвольными данными, форматирование съемных носителей
- Т10 - Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:
  - Т10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках
  - Т10.8. Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей

Указанные тактики и техники доступны для данного нарушителя.

⇨ УБИ$_3$ актуальна

$УБИ_4$ = [Разработчики программных, программно-аппаратных средств; АРМ работника отдела по работе с учениками; Использование уязвимостей конфигурации системы программного обеспечения; Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) и Потеря конкурентного преимущества.]

Сценарий реализации:

- Т1 - Сбор информации о системах и сетях:
  - Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
  - Т1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях - идентификационной информации пользователей
  - Т1.12. Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами
- Т3 - Внедрение и исполнение вредоносного программного обеспечения в системах и сетях:
  - Т3.6. Автоматическое создание вредоносных скриптов при помощи доступного инструментария от имени пользователя в системе с использованием его учетных данных
- Т6 - Повышение привилегий по доступу к компонентам систем и сетей:
  - Т6.7. Использование уязвимостей конфигурации системы, служб и приложений, в том числе

предварительно сконфигурированных профилей привилегированных пользователей, автоматически запускаемых от имени привилегированных пользователей скриптов, приложений и экземпляров окружения, позволяющих вредоносному ПО выполняться с повышенными привилегиями.

- Т7 - Сокрытие действий и применяемых при этом средств от обнаружения:
  - Т7.4. Отключение средств защиты от угроз информационной безопасности, в том числе средств антивирусной защиты, механизмов аудита, консолей оператора мониторинга и средств защиты других типов
- Т10 - Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:
  - Т10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках
  - Т10.7. Подмена информации (например, платежных реквизитов) в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей

Указанные тактики и техники доступны для данного нарушителя.

⇨ УБИ$_4$ актуальна

$УБИ_5$ = [Уборщица, недавно начала работу в организации (Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)); Линия связи между администратором и бухгалтерией; Повреждение LAN-кабеля (Механические повреждения); Необходимость дополнительных (незапланированных) затрат на восстановление деятельности и Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).]

Сценарий реализации:

- T10 - Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям
  - T10.10. Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети

Указанные тактики и техники доступны для данного нарушителя.

⇨ $УБИ_5$ актуальна

$УБИ_6$ = [хакер Ivan (Отдельные физические лица (хакеры)); Электронный почтовый ящик администратора; Кража персональных данных сотрудника; Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) и Срыв запланированной сделки с партнером]

Сценарий реализации:

- T1 - Сбор информации о системах и сетях:
  - T1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях - идентификационной информации пользователей
  - T1.9. Сбор информации о пользователях, устройствах, приложениях путем поиска информации в памяти, файлах, каталогах, базах данных, прошивках устройств, репозиториях исходных кодов ПО, включая поиск паролей в исходном и хэшированном виде, криптографических ключей.
- T2 - Получение первоначального доступа к компонентам систем и сетей:
  - T2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет)
  - T2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке
  - T2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы
- T7 - Сокрытие действий и применяемых при этом средств от обнаружения:
  - T7.1. Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения.

- T10 - Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:
    - T10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках
    - T10.7. Подмена информации (например, платежных реквизитов) в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей

Указанные тактики и техники доступны для данного нарушителя.

⇨ $УБИ_6$ актуальна

$УБИ_7$ = [Сотрудник другой автошколы, находящейся неподалеку (Конкурирующие организации); АРМ администратора; внедрение вредоносного ПО; Срыв запланированной сделки с партнером, Потеря клиентов, Потеря конкурентного преимущества и Утрата доверия]

Сценарий реализации:

- T1 - Сбор информации о системах и сетях:
    - T1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
    - T1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях - идентификационной информации пользователей
- T2 - Получение первоначального доступа к компонентам систем и сетей:

- T2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет)
- T2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке
- T2.4. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке

- T6 - Повышение привилегий по доступу к компонентам систем и сетей:
  - T6.2. Подбор пароля или другой информации для аутентификации от имени привилегированной учетной записи
- T7 - Сокрытие действий и применяемых при этом средств от обнаружения:
  - T7.1. Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения.
  - T7.2. Очистка/затирание истории команд и журналов регистрации, перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей
- T10 - Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:
  - T10.7. Подмена информации (например, платежных реквизитов) в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей

Указанные тактики и техники доступны для данного нарушителя.

⇨ УБИ$_7$ актуальна

УБИ$_8$ = [Поставщики вычислительных услуг, услуг связи; АРМ работника автопарка; Повреждение устройства связи (Механические повреждения); Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)]

Сценарий реализации:

- Т7 - Сокрытие действий и применяемых при этом средств от обнаружения:
  - Т7.5. Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса
  - Т7.7. Подделка данных телеметрии, данных вывода автоматизированных систем управления, данных систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса, данных видеонаблюдения и других визуально или автоматически интерпретируемых данных
- Т10 - Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:
  - Т10.3. Несанкционированное воздействие на программные модули прикладного программного обеспечения
  - Т10.10. Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети

Указанные тактики и техники доступны для данного нарушителя.

⇨ $УБИ_8$ актуальна

$УБИ_9$ = [Лица, обеспечивающие поставку программных, программно- аппаратных средств, обеспечивающих систем; Линия связи между инструктором и автопарком; Использование радиоэлектронных волновых генераторов для нарушения целостности передаваемой информации; Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)]

Сценарий реализации:

- T1 - Сбор информации о системах и сетях:
  - T1.2. Сбор информации о подключенных к публичным системам и сетям устройствах и их службах при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений.
- T2 - Получение первоначального доступа к компонентам систем и сетей:
  - T2.2. Использование устройств, датчиков, систем, расположенных на периметре или вне периметра физической защиты объекта, для получения первичного доступа к системам и компонентам внутри этого периметра.
- T7 - Сокрытие действий и применяемых при этом средств от обнаружения:
  - T7.5. Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса
- T10 - Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:

- T10.2. Несанкционированное воздействие на системное программное обеспечение, его конфигурацию и параметры доступа

Указанные тактики и техники доступны для данного нарушителя.

⇨ УБИ$_9$ актуальна

УБИ$_{10}$ = [Бывшие работники (пользователи); телефон инструктора для связи с учениками; Умышленное повреждение устройства (Механические повреждения); Нарушение деловой репутации и Необходимость дополнительных затрат на закупку товаров, работ или услуг (в том числе закупка ПО, технических средств, вышедших из строя, замена, настройка, ремонт, указанных средств)]

Сценарий реализации:

- T2 - Получение первоначального доступа к компонентам систем и сетей:
  - T2.14. Доступ путем эксплуатации недостатков систем биометрической аутентификации
- T7 - Сокрытие действий и применяемых при этом средств от обнаружения:
  - T7.5. Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса
- T10 - Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:
  - T10.3. Несанкционированное воздействие на программные модули прикладного программного обеспечения

- T10.10. Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети

Указанные тактики и техники доступны для данного нарушителя.

⇨ $УБИ_{10}$ актуальна

$УБИ_{11}$ = [Инструктор из другой автошколы (Отдельные физические лица (хакеры)); Основное устройство работы инструктора, связи с учениками; Внедрение вредоносного ПО, использование уязвимостей; Срыв запланированной сделки с партнером и Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)]

Сценарий реализации:

- T1 - Сбор информации о системах и сетях:
  - T1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
- T2 - Получение первоначального доступа к компонентам систем и сетей:
  - T2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет)
  - T2.5. Эксплуатация уязвимостей компонентов систем и сетей при удаленной или локальной атаке.
- T6 - Повышение привилегий по доступу к компонентам систем и сетей
  - –

Реализация данной тактики требует использования новых (не документированных) уязвимостей или доступа к интерфейсу канала передачи данных, что противоречит категории, уровню возможностей нарушителя (вида) источника угрозы (уровень возможностей нарушителя Н1 позволяет ему использовать только известные уязвимости и инструменты).

Следовательно, указанные тактики и техники не доступны для данного нарушителя, продолжение реализации угрозы не представляется возможным.

⇨ $УБИ_{11}$ неактуальна

Определение мер защиты информации от актуальных угроз безопасности информации

Ребро	Свойство	УБИ$_i$	Категория мер защиты	Подробно
Автомобильный сервис => Бухгалтерия	Конфиденци-альность	УБИ$_1$	Программно-технические (Криптографические)	Шифрование хранящихся данных
Автопарк => Автомобильный сервис	Целостность Доступность	УБИ$_2$	Организационные (Административные)	Создание регламента действий сотрудников в случаях кибератак. Разработка должностных инструкций административной безопасности. Проверка проведенных работ и тестирование системы
Администратор => ГИБДД	Целостность Доступность Конфиденци-альность	УБИ$_3$	Программно-технические (Криптографические)	Установка Средств Антивирусной защиты (САВЗ). Шифрование передаваемых данных симметричным шифром и данных, хранящихся на АРМ сотрудника.
Администратор => Инструктор	Целостность Доступность	УБИ$_4$	Программно-технические (Криптографические)	Криптографическая защита канала передачи данных.

	Конфиденци-альность			Резервирование данных. Создание и использование системы обнаружения атак.
Администратор => Бухгалтерия	Целостность Доступность	$УБИ_5$	Организационные (Организационно-технические)	Защита LAN-сети от механических повреждений (изоляция проводки в труднодоступные места).
			Организационные (Административные)	Проведение инструктажа работников.
Ученик => Администратор	Конфиденци-альность	$УБИ_6$	Программно-технические	Использование системы обнаружения атак
			Организационные (Административные)	Обучение персонала действиям в случае кибератак, проведение тренировок по регламенту проведения аудита безопасности.
Администратор => Ученик	Целостность Доступность	$УБИ_7$	Программно-технические	Установка САВЗ
			Организационные (Административные)	Разработка и введение инструкции по использованию САВЗ

Автопарк => Инструктор	Целостность	$УБИ_8$	Организационные (Административные)	Разработка должностных инструкций административной безопасности. Проверка и тестирование работы систем связи.
Инструктор => Автопарк	Целостность	$УБИ_9$	Программно-технические	Проведение переговоров в отдельном помещении (и его защита), не доступном для посторонних лиц. (Экранирование)
			Организационные (Организационно-технические)	Установка пропускной системы.
Ученик => Инструктор	Конфиденци-альность	$УБИ_{10}$	Организационные (Организационно-технические)	Физическая защита средств коммуникации сотрудника. Защита поддерживаемой инфраструктуры.

Таблица 8. Меры защиты против активных угроз

Итоговый список всех мер защиты информации

- Организационные:
  - Административные:
    - Создание регламента действий сотрудников в случаях кибератак.
    - Разработка должностных инструкций административной безопасности.
    - Проверка проведенных работ и тестирование системы.
    - Проведение инструктажа работников.
    - Обучение персонала действиям в случае кибератак, проведение тренировок по регламенту проведения аудита безопасности.
    - Разработка и введение инструкции по использованию САВЗ
  - Организационно-технические:
    - Защита LAN-сети от механических повреждений (изоляция проводки в труднодоступные места).
    - Установка пропускной системы.
    - Физическая защита средств коммуникации сотрудника.
    - Защита поддерживаемой инфраструктуры.
- Программно-технические:
  - Криптографические:
    - Шифрование передаваемых данных симметричным шифром и данных, хранящихся на АРМ сотрудника.
    - Криптографическая защита канала передачи данных.
    - Резервирование данных.
    - Создание и использование системы обнаружения атак.
  - Техническая защита:
    - Установка Средств Антивирусной защиты (САВЗ).

- Проведение переговоров в отдельном помещении (и его защита), не доступном для посторонних лиц. (Экранирование)
- Использование системы обнаружения атак