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	3
Объект информатизации2	1
Способы передачи данных5	5
Определение свойств информации, которые необходимо обеспечить	7
Определение возможных негативных последствий от реализации угроз безопасность информации12	
Определение объектов воздействия и видов воздействия на них 14	1
Определение источников угроз безопасности информации20)
Определение способов реализации (возникновения) угроз безопасности информации31	1
Определение угроз безопасности информации37	7
Определение перечня актуальных угроз безопасности информации)
Определение мер защиты информации от актуальных угроз безопасности информации56	5
Итоговый список всех мер защиты информации59)

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

Автошкола "Возьми и сдай"

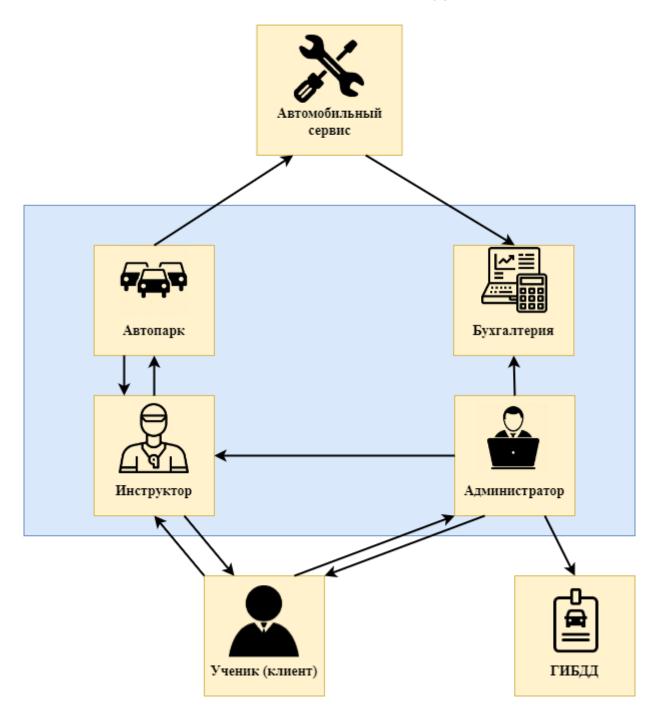


Рисунок 1. Объект информатизации

Способы передачи данных

Локальная сеть	
Мобильная связь	
Речь	δ
Письмо по почте	

Таблица 1. Обозначения способов передачи данных

Автошкола "Возьми и сдай"

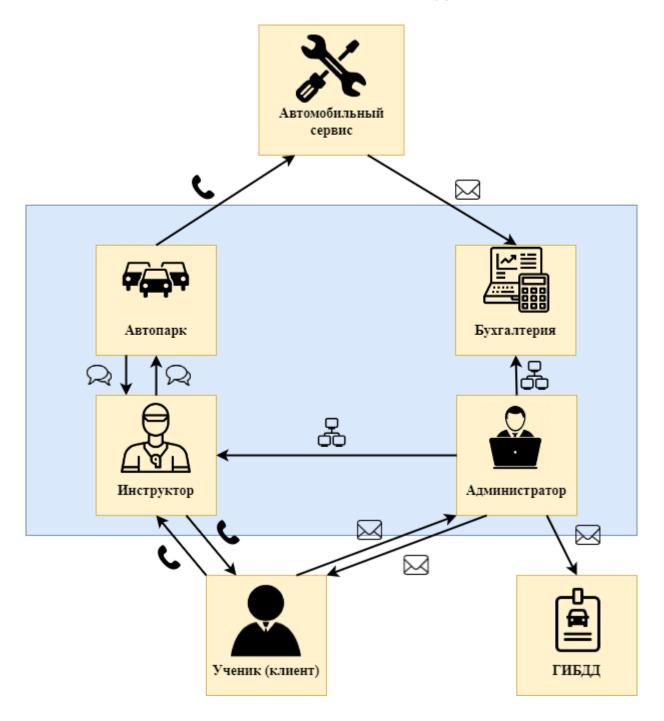


Рисунок 2. Способы передачи данных

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.	Конфиденциальность можно не обеспечивать так как данная информация общедостпная

4	Администратор => Бухгалтерия	Локальная сеть	Передача информации об учениках	3. Доступность Беспрепятственная реализация права доступа инструктора на информацию 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 Доступность обеспечивает не отдел информаци-
5	Ученик => Администратор	Письмо по почте	Передача персональных данных	1. Конфиденциальность Обеспечение приватности персональных данных учеников.	информаци- онной безопасности объекта информати- зации

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

	Автопарк		Передача	1. Целостность	информаци- онной безопасности объекта информати- зации. Конфиденци- альность можно не обеспечивать так как
9	=> Инструктор	Речь	информации о свободных автомобилях	Неизменность передаваемых данных.	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.

Автошкола "Возьми и сдай"

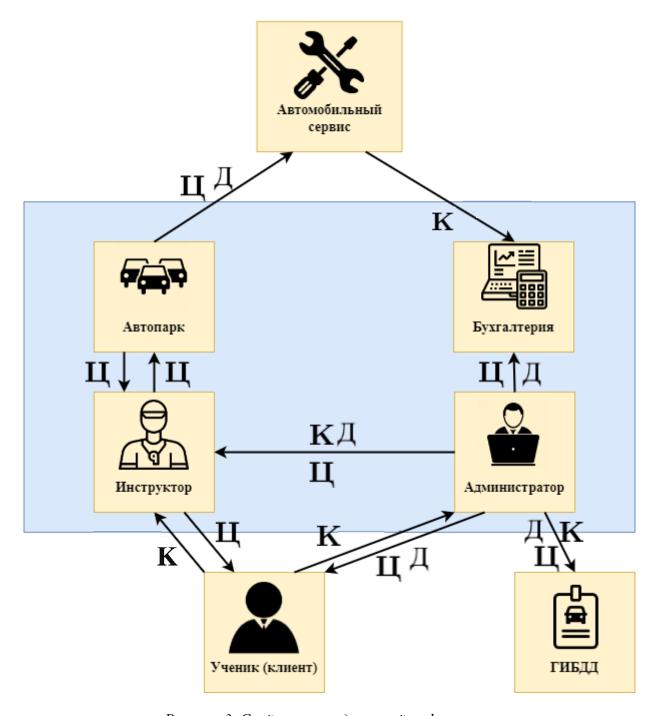


Рисунок 3. Свойства передаваемой информации

Определение возможных негативных последствий от реализации угроз безопасность информации

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

Потеря (хищение) денежных средств. Риски юридическому лицу, Необходимость дополнительных индивидуальному (незапланированных) затрат на выплаты предпринимателю, связанные с хозяйственной штрафов (неустоек) или компенсаций. Необходимость дополнительных затрат на деятельностью 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

Потеря клиентов.

Потеря конкурентного преимущества. Невозможность заключения договоров, соглашений.

Нарушение деловой репутации.

восстановление деятельности.

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	Объекты воздействия	Виды воздействия
	последствия		
	Нарушение тайны	Электронный	Утечка
	переписки,	почтовый ящик	идентификационной
	телефонных	администратора.	информации граждан.
	переговоров, иных		
	сообщений.		
	Финансовый,	Удаленное	Утечка реквизитов
	иной	автоматизированное	платежных поручений
	материальный	место (АРМ)	граждан с АРМ работника
	ущерб	работника отдела по	отдела по работе с
У1	физическому	работе с учениками.	учениками.
	лицу.		
	Нарушение	Удаленное	Утечка
	конфиденциальност	автоматизированное	идентификационной
	и(утечка)	место (АРМ)	информации и
	персональных	оператора отдела по	персональных данных
	данных.	работе с клиентами.	граждан с АРМ работника
			отдела по работе с
			учениками.

	Разглашение персональных данных.	Удаленное автоматизированное место (APM) оператора отдела по работе с клиентами.	Утечка идентификационной информации и персональных данных граждан с APM работника отдела по работе с учениками.
	Потеря (хищение) денежных средств.	АРМ финансового директора (бухгалтерия).	Несанкционированная модификация информации в платежных распоряжениях и отправка недостоверных распоряжений от имени финансового директора.
У2		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 APM главного бухгалтера.

	Необходимость	Удаленное	Утечка реквизитов
	дополнительных	автоматизированное	платежных поручений
	(незапланированных	место (АРМ)	граждан с АРМ
) затрат на выплаты	работника отдела по	оператора.
	штрафов (неустоек)	работе с учениками.	The state of the s
	или компенсаций.	,	
-	Необходимость	Линия связи между	Подмена данных,
	дополнительных	автоинструктором и	содержащих информацию
	затрат на закупку	автомобильным	о нужном автомобиле и
	товаров, работ или	парком.	времени его выдачи.
	услуг (в том числе	1	1
	закупка ПО,		
	технических		
	средств, вышедших		
	из строя, замена,		
	настройка, ремонт,		
	указанных средств).		
-	Срыв	АРМ работника отдела	Модификация
	запланированной	по работе с учениками.	информации и отправка
	сделки с партнером.		данных с недостоверной
			информацией от имени
			работника отдела по
			работе с учениками.
		Электронный	Модификация
		почтовый ящик	информации и отправка
		работника отдела по	электронных писем с
		работе с учениками.	недостоверной
			информацией от имени
			работника отдела по
<u></u>			работе с учениками.
	Необходимость	АРМ сотрудника	Несанкционированная
	дополнительных	автомобильного парка.	модификация
	(незапланированных		информации по
) затрат на		состоянию и ремонту
	восстановление		автомобилей.
	деятельности.		

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	АРМ сотрудника	Утечка приватной
конкурентного	автомобильного парка.	информации о
преимущества.		сотрудничестве с
		определенным
		автомобильным
		сервисом.
Невозможность	АРМ администратора.	Отказ в обслуживании
заключения		сайта и других систем
договоров,		связи. Внедрение
соглашений.		вредоносного ПО с целью
		нарушения работы сайта
		и других систем связи.
Нарушение деловой	АРМ администратора.	Отказ в обслуживании
репутации.		сайта и других систем
		связи. Внедрение
		вредоносного ПО с целью
		нарушения работы сайта
		и других систем связи.
	АРМ сотрудника	Утечка приватной
	автомобильного парка.	информации о
		сотрудничестве с
		определенным
		автомобильным
		сервисом.
Снижение престижа.	АРМ работника отдела	Модификация
	по работе с учениками.	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	Утечка приватной
	автомобильного парка.	информации о
		сотрудничестве с
		определенным
		автомобильным
		сервисом.
Причинение	АРМ сотрудника	Механическое
имущественного	компании.	повреждение.
ущерба.		
Невозможность	АРМ сотрудника	Несанкционированная
решения задач	автомобильного парка.	модификация
(реализации		информации по
функций) или		состоянию и ремонту
снижение		автомобилей.
эффективности		
решения задач		
(реализации		
функций).		
Утечка	АРМ сотрудника	Внедрение вредоносного
конфиденциальной	компании.	ПО с целью получения
информации		

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

Таблица 4. Определение объектов воздействия и видов воздействия на них

Определение источников угроз безопасности информации

Виды	Возможны	Возможные цели реализации угроз		Соответствие целей видам
нарушител	безопасно	сти информации		риска (ущерба) и
ей	У1	У2	У3	возможным негативным
				последствиям
Специальн				
ые службы				
иностранн				
ых	_	-	_	-
государств				
Террорист				
ические,				
экстремис				
тские	_	_	_	-
группиров				
ки				
Преступн	+	+		У1
ые группы	(получен	(Получение		(Финансовый, иной
(криминал	ие	финансовой		материальный ущерб
ьные	финансов	выгоды за счет		физическому лицу.
структуры	ой	кражи и		Нарушение
)	выгоды	коммерческой		конфиденциальности(утечк
	за счет	тайны.		а) персональных данных.)
	кражи и	Желание		
	продажи	самореализаци	-	У2
	персонал	и)		(Потеря (хищение)
	ьных			денежных средств.
	данных			Необходимость
	граждан)			дополнительных
				(незапланированных) затрат
				на выплаты штрафов
				(неустоек) или
				компенсаций.

	<u> </u>	T	T
			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) затра
			на восстановление
			деятельности.
			Нарушение деловой
			репутации.
			Причинение
			имущественного ущерба.
			Утечка конфиденциальной
			информации (коммерческой
			тайны, секретов
			производства (ноу-хау) и
			др.))
Отдельны	+	+	У1
e	(получен	(получение	(Нарушение тайны
физически	ие	финансовой	переписки, телефонных
е лица	финансов	выгоды за счет	переговоров, иных
(хакеры)	ой	кражи и	сообщений.
	выгоды	коммерческой	Финансовый, иной
	за счет	тайны.	- материальный ущерб
	кражи и	желание	физическому лицу.
	продажи	самореализаци	Нарушение
	персонал	и)	конфиденциальности(утечк
	ьных		а) персональных данных.)
	данных		
	граждан)		У2

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

Разработч	+	У2
ики	(Получение	(Потеря конкурентного
программн	конкурентных	преимущества.
ых,	преимуществ.	Причинение
программн	получение	имущественного ущерба.
0-	- финансовой	Утечка конфиденциальной
аппаратны	выгоды за счет	информации (коммерческой
х средств	кражи и	тайны, секретов
	коммерческой	производства (ноу-хау) и
	тайны)	др.))
Лица,	+	У2
обеспечив	(получение	(Потеря (хищение)
ающие	финансовой	денежных средств.
поставку	выгоды за счет	Потеря клиентов.
программн	кражи и	Потеря конкурентного
ых,	коммерческой	преимущества.
программн	тайны.	Причинение
O-	Непреднамерен	имущественного ущерба.
аппаратны	ные,	Утечка конфиденциальной
х средств,	- неосторожные	- информации (коммерческой
обеспечив	или	тайны, секретов
ающих	неквалифициро	производства (ноу-хау) и
систем	ванные	др.)
	действия.	Невозможность решения
	Получение	задач (реализации функций)
	конкурентных	или снижение
	преимуществ.)	эффективности решения
		задач (реализации
		функций)))

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

		Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.))
Лица,	+	У2
обеспечив	(получение	(Необходимость
ающие	финансовой	дополнительных
функцион	выгоды за счет	(незапланированных) затрат
ирование	кражи и	на восстановление
систем и	коммерческой	деятельности.
сетей или	тайны.	Причинение
обеспечив	Непреднамерен	имущественного ущерба.
ающие	ные,	Невозможность решения
системы	- неосторожные	- задач (реализации функций)
оператора	или	или снижение
(админист	неквалифициро	эффективности решения
рация,	ванные	задач (реализации
охрана,	действия)	функций).
уборщики		Утечка конфиденциальной
и т.д.)		информации (коммерческой
		тайны, секретов
		производства (ноу-хау) и
		др.))

Авторизов		+	У2
анные		(получение	(Потеря (хищение)
пользовате		финансовой	денежных средств.
ли систем		выгоды за счет	Необходимость
и сетей		кражи и	дополнительных затрат на
		коммерческой	закупку товаров, работ или
		тайны.	услуг (в том числе закупка
		Любопытство	ПО, технических средств,
		или желание	вышедших из строя, замена,
		самореализаци	настройка, ремонт,
	_	И	указанных средств). Срыв
		Месть за ранее	запланированной сделки с
		совершенные	партнером.
		действия.	Причинение
		Непреднамерен	имущественного ущерба.
		ные,	Утечка конфиденциальной
		неосторожные	информации (коммерческой
		или	тайны, секретов
		неквалифициро	производства (ноу-хау) и
		ванные	др.))
		действия)	др.))
Системны	+	+	У1
е	(Месть за	(получение	(Разглашение персональных
администр	ранее	финансовой	данных.)
аторы и	1	выгоды за счет	данных.)
_	ные		У2
администр аторы	действия.	кражи и коммерческой	(Потеря (хищение)
безопасно	денетвил.	тайны.	денежных средств.
сти	/	Любопытство -	Срыв запланированной
СТИ		или желание	сделки с партнером.
			Потеря клиентов.
		самореализаци и.	Потеря конкурентного
		Месть за ранее	преимущества.
		-	Нарушение деловой
		совершенные действия.	
		деиствия.	репутации.
			Утрата доверия.

	1	<u>, </u>		
		Непреднамерен		Причинение
		ные,		имущественного ущерба.)
		неосторожные		
		или		
		неквалифициро		
		ванные		
		действия.)		
Бывшие	+	+		У1
работники	(Месть за	(получение		(Нарушение тайны
(пользоват	ранее	финансовой		переписки, телефонных
ели)	совершен	выгоды за счет		переговоров, иных
	ные	кражи и		сообщений.
	действия.	коммерческой		Разглашение персональных
)	тайны.		данных.)
		Месть за ранее		
		совершенные		У2
		действия.)		(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.
		1		<u> </u>

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	Отдельные физические лица (хакеры)	Внешний	H1
переговоров, иных сообщений. Финансовый,	Бывшие работники (пользователи)	Внешний	H1
иной материальный ущерб физическому лицу. Нарушение конфиденциальности(утечка)	Преступные группы (криминальные структуры)	Внешний	H2
персональных данных. Разглашение персональных данных.	Системные администраторы и администраторы безопасности	Внутренний	H2
	Конкурирующие организации	Внешний	H2
	Лица, обеспечивающие поставку программных, программно- аппаратных средств, обеспечивающих систем	Внешний	H1
	Поставщики вычислительных услуг, услуг связи	Внутренний	H2
	Авторизованные пользователи систем и сетей	Внутренний	H1

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

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

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

Определение способов реализации (возникновения) угроз безопасности информации

Nº	Вид нарушите ля	Категория нарушител я	Объект воздействи я	Доступные интерфейсы	Способы реализации
1	Преступн ые группы (криминал ьные структуры) (H2)	внешний	Удаленное автоматизи рованное место (АРМ) работника отдела по работе с учениками. АРМ финансовог о директора (бухгалтер ия).	Доступ через LAN-сеть организации	Внедрение вредоносного ПО (программного обеспечения)
2	Отдельны е физически е лица (хакеры) (H1)	внешний	Удаленное автоматизи рованное место (АРМ) работника отдела по работе с учениками. Электронный почтовый ящик финансовог	Рассылка писем с фишингом	Кража персональных данных сотрудника, ввиду его непрофессиона лизма и внедрение вредоносного ПО и получение удаленного доступа к APM сотрудника

			о директора.		
3	Конкурир ующие организац ии (H2)	внешний	(АРМ) работника отдела по работе с учениками. АРМ сотрудника автомобиль	Доступ через LAN-сеть организации	Внедрение вредоносного ПО
			ного парка. Электронный почтовый ящик финансовог о директора. Электронный почтовый ящик администра тора.	Рассылка фишинговых писем	Кража персональных данных сотрудника и владеемой им информацией.
4	Разработч ики программ ных, программ но- аппаратны х средств (Н3)	внутренний	Удаленное автоматизи рованное место (АРМ) работника отдела по работе с учениками.	Доступ через LAN-сеть организации	Внедрение вредоносного ПО

			АРМ сотрудника автомобиль ного парка. АРМ финансовог о директора (бухгалтер	Съемные машинные носители информации, подключаемые к APM сотрудника	Использование уязвимостей конфигурации системы программного обеспечения
5	Поставщи ки вычислите льных услуг,	внешний	ия). Удаленное автоматизи рованное место (APM)	Неосторожность или непрофессионал изм данных лиц	Механические повреждения.
	услуг связи (Н2)		работника отдела по работе с учениками.	Съемные машинные носители информации, подключаемые к APM сотрудника	Использование уязвимостей конфигурации APM сотрудника
6	Лица, привлекае мые для установки, настройки , испытани й,	внутренний	АРМ главного бухгалтера. АРМ	Съемные машинные носители информации, подключаемые к APM сотрудника	Внедрение вредоносного ПО Использование уязвимостей конфигурации APM сотрудника
	пусконала дочных и иных		АРМ сотрудника автомобиль ного парка.	Неосторожность или непрофессионал изм данных лиц	Механические повреждения.

			A DN (
	видов		APM		
	работ (Н2)		работника		
			отдела по		
			работе с		
			учениками.		
7	Лица,	внешний	APM	Поставка	Использование
	обеспечив		работника	программных,	уязвимостей
	ающие		автопарка.	программно-	кода ПО
	поставку			аппаратных	
	программ			средств,	
	ных,			обеспечивающ	
	программ			их систем с	
	но-			уязвимостями	
	аппаратны			В	
	х средств,			коде	
	обеспечив				
	ающих				
	систем				
	(H2)				
8	Лица,	внутренний	APM	Неосторожность	Механические
	обеспечив		работника	или	повреждения.
	ающие		отдела по	непрофессионал	
	функцион		работе с	изм данных лиц	
	ирование		учениками.	при работе с	
	систем и			соответствующи	
	сетей или			м инвентарем	
	обеспечив		APM	Съемные	Дублирование
	ающие		главного	машинные	приватной
	системы		бухгалтера.	носители	информации
	оператора			информации,	на
	(админист			подключаемые	съемные

	рация, охрана, уборщики и т.д.) (H1)		АРМ сотрудника автомобиль ного парка.	к АРМ сотрудника	машинные носители информации
9	Системны е администр аторы и администр аторы безопасно сти (H2)	внутренний	АРМ главного бухгалтера.	Съемные машинные носители информации, подключаемые к APM сотрудника	Дублирование приватной информации на съемные машинные носители информации
10	Авторизов анные пользоват ели систем и сетей (H1)	внутренний	АРМ работника отдела по работе с учениками.	Неосторожность или непрофессионал изм данных лиц Съемные машинные носители информации, подключаемые к APM сотрудника	Механические повреждения Дублирование приватной информации на съемные машинные носители информации
11	Бывшие работники (пользоват ели) (H1)	внешний	Электронн ый почтовый ящик администра тора.	Рассылка фишинговых писем	Кража персональных данных сотрудника и владеемой им информацией.

		Умышленное	Механические
		нанесение	повреждения
		ущерба	_
		подручными	
		средствами	

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

Определение угроз безопасности информации

УБИ₁ = [Другая автошкола, находящаяся неподалеку (Конкурирующие организации); APM работника бухгалтерии; внедрение вредоносного ПО; Потеря конкурентного преимущества и Срыв запланированной сделки с партнером]

УБИ₂ = [Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ; APM 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)]

УБИ₃ = [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.)]

УБИ₄ = [Разработчики программных, программно-аппаратных средств; APM 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.]

УБИ₅ = [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).]

УБИ₆ = [хакер Ivan (Отдельные физические лица (хакеры)); Электронный почтовый ящик администратора; Кража персональных данных сотрудника; Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноухау) и др.) и Срыв запланированной сделки с партнером]

УБИ₇ = [Сотрудник другой автошколы, находящейся неподалеку (Конкурирующие организации); APM администратора; внедрение вредоносного ПО; Срыв запланированной сделки с партнером, Потеря клиентов, Потеря конкурентного преимущества и Утрата доверия]

УБИ₈ = [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)]

УБИ₉ = [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)]

УБИ₁₁ = [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

УБИ₁ = [Другая автошкола, находящаяся неподалеку (Конкурирующие организации); APM работника бухгалтерии; внедрение вредоносного ПО; Потеря конкурентного преимущества и Срыв запланированной сделки с партнером]

- ➤ 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
 - Т1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга
- ➤ Т2 Получение первоначального доступа к компонентам систем и сетей:
 - о T2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет)
 - Т2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке
 - Т2.4. 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:
 - о 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.

⇒ УБИ1 актуальна

УБИ $_2$ = [Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ; APM 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)]

- ➤ 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:
 - ТЗ.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
- ➤ T10 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.

⇒ УБИ2 актуальна

УБИ₃ = [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.)]

- ➤ 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:
 - о 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:
 - о T10.1. 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.

⇒ УБИ3 актуальна

УБИ₄ = [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.]

- ➤ 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:
 - о 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:
 - о 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.

⇒ УБИ4 актуальна

УБИ₅ = [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
 - Т10.10. Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети

Указанные тактики и техники доступны для данного нарушителя.

⇒ УБИ5 актуальна

УБИ₆ = [хакер Ivan (Отдельные физические лица (хакеры)); Электронный почтовый ящик администратора; Кража персональных данных сотрудника; Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноухау) и др.) и Срыв запланированной сделки с партнером]

- ➤ Т1 Сбор информации о системах и сетях:
 - 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
 - Т1.9. 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.
- ➤ Т2 Получение первоначального доступа к компонентам систем и сетей:
 - Т2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет)
 - Т2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей 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
- ▶ 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.

- ➤ Т10 Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям:
 - о T10.1. 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.

⇒ УБИ₆ актуальна

УБИ₇ = [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]

- ➤ Т1 Сбор информации о системах и сетях:
 - о 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:

- о T2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет)
- Т2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке
- Т2.4. 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
- ➤ Т6 Повышение привилегий по доступу к компонентам систем и сетей:
 - о 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
- ➤ T10 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.

⇒ УБИ7 актуальна

УБИ₈ = [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
 - о T10.10. Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети

Указанные тактики и техники доступны для данного нарушителя.

⇒ УБИ8 актуальна

УБИ₉ = [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)]

- ➤ Т1 Сбор информации о системах и сетях:
 - Т1.2. 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.
- ➤ Т2 Получение первоначального доступа к компонентам систем и сетей:
 - Т2.2. Использование устройств, датчиков, систем, расположенных на периметре или вне периметра физической защиты объекта, для получения первичного доступа к системам и компонентам внутри этого периметра.
- ➤ 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
- ➤ T10 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.

⇒ УБИ9 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)]

- ➤ Т2 Получение первоначального доступа к компонентам систем и сетей:
 - о T2.14. Доступ путем эксплуатации недостатков систем биометрической аутентификации
- ➤ 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
- ➤ 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.

⇒ УБИ₁₀ актуальна

УБИ₁₁ = [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:

- ➤ 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
- ➤ Т2 Получение первоначального доступа к компонентам систем и сетей:
 - Т2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет)
 - о T2.5. Эксплуатация уязвимостей компонентов систем и сетей при удаленной или локальной атаке.
- ▶ Т6 Повышение привилегий по доступу к компонентам систем и сетей

0 -

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.

⇒ УБИ₁₁ неактуальна

Определение мер защиты информации от актуальных угроз безопасности информации

Ребро	Свойство	УБИі	Категория мер	Подробно
	TO 1	XXDXX	защиты	*** 1
Автомобильный	Конфиденци-	УБИ1	Программно-	Шифрование
сервис	альность		технические	хранящихся
=> Бухгалтерия			(Криптографические)	данных
Автопарк	Целостность	УБИ2	Организационные	Создание
=>	Доступность		(Административные)	регламента
Автомобильный				действий
сервис				сотрудников в
				случаях кибератак.
				Разработка
				должностных
				инструкций
				административной
				безопасности.
				Проверка
				проведенных работ
				и тестирование
				системы
Администратор	Целостность	УБИ3	Программно-	Установка Средств
=>	Доступность		технические	Антивирусной
ГИБДД	Конфиденци-		(Криптографические)	защиты (САВЗ).
	альность			Шифрование
				передаваемых
				данных
				симметричным
				шифром и данных,
				хранящихся на
				АРМ сотрудника.
Администратор	Целостность	УБИ4	Программно-	Криптографическая
=>	Доступность		технические	защита канала
Инструктор			(Криптографические)	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
			Организационные	труднодоступные места). Проведение
			(Административные)	инструктажа работников.
Ученик => Администратор	Конфиденци- альность	УБИ ₆	Программно- технические Организационные	Использование системы обнаружения атак Обучение
			(Административные)	персонала действиям в случае кибератак, проведение
				тренировок по регламенту проведения аудита безопасности.
Администратор =>	Целостность Доступность	УБИ7	Программно- технические	Установка САВЗ
Ученик			Организационные (Административные)	Разработка и введение инструкции по использованию CAB3

	Целостность	УБИ8	Организационные	Разработка
			(Административные)	должностных
				инструкций
Автопарк				административной
=>				безопасности.
Инструктор				Проверка и
				тестирование
				работы систем
				связи.
	Целостность	УБИ9	Программно-	Проведение
			технические	переговоров в
				отдельном
				помещении (и его
Инструктор				защита), не
=>				доступном для
Автопарк				посторонних лиц.
				(Экранирование)
			Организационные	Установка
			(Организационно-	пропускной
			технические)	системы.
Ученик	Конфиденци-	УБИ ₁₀	Организационные	Физическая защита
=>	альность		(Организационно-	средств
Инструктор			технические)	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 CAB3
 - > 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 APM 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