

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ГЕОДЕЗИИ И  
КАРТОГРАФИИ

Отчет по практической работе

«ФСТЭК»

Выполнил:

Студент ФГиИБ ИБЗ-16

Кузичев Дмитрий Александрович

Руководитель:

Преподаватель

Сверлов Егор Дмитриевич

Таблица 1

	Наименование	Эксперт Напольских	Эксперт Кузичев	Эксперт Зими́на
У1	Угроза жизни или здоровью			
У1	Унижение достоинства личности			
У1	Нарушение свободы, личной неприкосновенности	Низкая		
У1	Нарушение неприкосновенности частной жизни	Средняя	Низкая	Низкая
У1	Нарушение личной, семейной тайны, утрата чести и доброго имени		Низкая	Низкая
У1	Нарушение тайны переписки, телефонных переговоров, иных сообщений			
У1	Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах			
У1	Финансовый, иной материальный ущерб физическому лицу	Низкая	Средняя	Низкая
У1	Нарушение конфиденциальности (утечка) персональных данных			
У1	«Травля» гражданина в сети «Интернет»	Средняя	Низкая	Низкая
У1	Разглашение персональных данных граждан			
У2	Нарушение законодательства Российской Федерации	Низкая	Низкая	Низкая
У2	Потеря (хищение) денежных средств			
У2	Недополучение ожидаемой (прогнозируемой) прибыли			
У2	Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций	Высокая	Высокая	Низкая

У2	Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств)	Средняя	Низкая	Низкая
----	---	---------	--------	--------

У2	Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса	Низкая	Низкая	Низкая
У2	Срыв запланированной сделки с партнером			
У2	Необходимость дополнительных (незапланированных) затрат на восстановление деятельности	Средняя	Низкая	Низкая
У2	Потеря клиентов, поставщиков.			
У2	Потеря конкурентного преимущества			Низкая
У2	Невозможность заключения договоров, соглашений			
У2	Нарушение деловой репутации. Снижение престижа	Высокая		Средняя
У2	Дискредитация работников			
У2	Утрата доверия			
У2	Причинение имущественного ущерба	Низкая	Высокая	Средняя
У2	Неспособность выполнения договорных обязательств			
У2	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)			
У2	Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций)	Средняя	Низкая	Высокая

У2	Принятие неправильных решений			
У2	Простой информационной системы или сети	Низкая	Средняя	Средняя
У2	Публикация недостоверной информации на веб-ресурсах организации	Высокая	Средняя	Низкая
У2	Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением			
У2	Рассылка информационных сообщений с использованием вычислительных мощностей			

	оператора и (или) от его имени			
У2	Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)	Низкая	Средняя	Низкая
У3	Причинение ущерба жизни и здоровью людей.			
У3	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения			
У3	Прекращение или нарушение функционирования объектов транспортной инфраструктуры			
У3	Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)			
У3	Прекращение или нарушение функционирования сети связи			
У3	Отсутствие доступа к государственной услуге			

УЗ	Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации			
УЗ	Снижение уровня дохода государственной корпорации, государственной организации или организации с государственным участием	Низкая	Низкая	Низкая
УЗ	Возникновение ущерба бюджетам Российской Федерации.			
УЗ	Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций в			

	системно значимой кредитной организации, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем, системно значимой инфраструктурной организацией финансового рынка			
УЗ	Вредные воздействия на окружающую среду			
УЗ	Прекращение или нарушение функционирования пункта управления (ситуационного центра).			
УЗ	Снижение показателей государственного оборонного заказа.			
УЗ	Прекращение или нарушение функционирования информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка			

УЗ	Нарушение законодательства Российской Федерации	Низкая	Низкая	Высокая
УЗ	Публикация недостоверной социально значимой информации на веб-ресурсах, которая может привести к социальной напряженности, панике среди населения и др.	Низкая	Низкая	Средняя
УЗ	Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса, если это ведет к выводу из строя технологических объектов, их компонентов.			
УЗ	Нарушение общественного порядка, возможность потери или снижения уровня контроля за общественным порядком.	Низкая	Низкая	Низкая
УЗ	Нарушение выборного процесса	Низкая	Средняя	Средняя
УЗ	Отсутствие возможности оперативного оповещения населения о чрезвычайной ситуации			
УЗ	Организация пикетов, забастовок, митингов и других акций	Низкая	Низкая	Низкая
УЗ	Массовые увольнения			
УЗ	Увеличение количества жалоб в органы государственной власти или органы местного самоуправления	Низкая	Низкая	Высокая
УЗ	Появление негативных публикаций в общедоступных источниках	Средняя	Низкая	Низкая
УЗ	Создание предпосылок к внутривнутриполитическому кризису			

УЗ	Доступ к персональным данным сотрудников органов государственной власти, уполномоченных в области обеспечения обороны, безопасности и правопорядка, высших должностных лиц государственных органов и других лиц государственных органов.			
УЗ	Доступ к системам и сетям с целью незаконного использования вычислительных мощностей			
УЗ	Использование веб-ресурсов государственных органов для распространения и управления вредоносным программным обеспечением			
УЗ	Утечка информации ограниченного доступа	Высокая	Высокая	Высокая
УЗ	Непредоставление государственных услуг			

Таблица 2

№	Виды риска (ущерба)	Возможные типовые негативные последствия
У1	Ущерб физическому лицу	Унижение достоинства личности. Нарушение тайны переписки, телефонных переговоров, иных сообщений.
У2	Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью	Недополучение ожидаемой прибыли. Необходимость дополнительных затрат на выплаты штрафов или компенсаций. Необходимость дополнительных затрат на закупку товаров, работ или услуг. Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса.
У3	Ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	Публикации с призывом к терроризму и экстремизму  Публикации, разглашающие государственную тайну



Таблица 3

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	
Террористические, экстремистские группировки	+	+	+	У2 (необходимость дополнительных затрат на восстановление деятельности; простой информационной системы или сети)
Преступные группы (криминальные структуры)	-	-	-	У2 (невозможность решения задач или снижение эффективности решения задач)
Отдельные физические лица (хакеры)	+	+	-	У1 (унижение достоинства личности; «травля» гражданина в сети «Интернет»; нарушение конфиденциальности (утечка) персональных данных) У2 (использование вебресурсов для распространения и управления вредоносным программным

				обеспечением; необходимость дополнительных затрат на выплаты штрафов или компенсаций)
Конкурирующие организации	-	-	+	У2 (потеря клиентов, поставщиков) У3 (появление негативных публикаций в общедоступных источниках)
Разработчики программных, программноаппаратных средств	-	+	-	У2 (невозможность решения задач или снижение эффективности решения задач)
Лица, обеспечивающие поставку программных, программноаппаратных средств, обеспечивающих систем	-	+	-	У2 (неспособность выполнения договорных обязательств)
Поставщики вычислительных услуг, услуг связи	+	+	-	У2 (недополучение ожидаемой прибыли; потеря конкурентного преимущества; необходимость дополнительных затрат на

				закупку товаров, работ или услуг;)
--	--	--	--	---------------------------------------

Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	+	+	+	
Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	+	+	+	У2 (Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса; необходимость изменения внутренних процедур для достижения целей, решения задач) У3 (доступ к системам и сетям с целью незаконного использования вычислительных мощностей)
Авторизованные пользователи систем и сетей	-	-	-	У1 (разглашение персональных данных граждан) У2 (утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.))

Системные администраторы и администраторы безопасности	+	+	+	У2 (публикация недостоверной информации на веб-ресурсах организации)
--	---	---	---	---

Бывшие работники (пользователи)	-	-	-	У1 (нарушение неприкосновенности частной жизни; нарушение тайны переписки, телефонных переговоров, иных сообщений) У2 (снижение престижа; нарушение деловой репутации; утрата доверия)
------------------------------------	---	---	---	--

Таблица 4

№ п/п	Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
1	У1: унижение достоинства личности; нарушение неприкосновенности частной жизни; нарушение тайны переписки, телефонных переговоров, иных сообщений; нарушение конфиденциальности (утечка) персональных данных; «травля» гражданина в сети «Интернет»; разглашение персональных данных граждан	Отдельные физические лица (хакеры)	Внешний	Н1
		Авторизованные пользователи систем и сетей	Внутренний	Н1
		Бывшие работники (пользователи)	Внешний	Н1
2	У2: недополучение ожидаемой (прогнозируемой) прибыли; необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций; необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств); нарушение штатного режима функционирования автоматизированной системы управления и	Террористические, экстремистские группировки	Внешний	Н3
		Преступные группы (криминальные структуры)	Внешний	Н2
		Отдельные физические лица (хакеры)	Внешний	Н3
		Разработчики программных, программноаппаратных средств	Внутренний	Н3

	<p>управляемого объекта и/или процесса; необходимость дополнительных (незапланированных) затрат на восстановление деятельности;</p>			
--	---	--	--	--

	<p>потеря клиентов, поставщиков; потеря конкурентного преимущества; нарушение деловой репутации; снижение престижа; утрата доверия; неспособность выполнения договорных обязательств; невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций); необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций); простой информационной системы или сети; публикация недостоверной информации на веб-ресурсах организации; использование веб- ресурсов для распространения и управления вредоносным программным обеспечением</p>	Лица, обеспечивающие поставку программных, программноаппаратных средств, обеспечивающих систем	Внешний	H1
		Поставщики вычислительных услуг, услуг связи	Внутренний	H2
		Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Внутренний	H1
		Авторизованные пользователи систем и сетей	Внутренний	H2
		Системные администраторы и администраторы безопасности	Внутренний	H2
		Бывшие работники (пользователи)	Внешний	H1

3	УЗ: появление негативных публикаций в общедоступных источниках; доступ к системам и сетям с целью незаконного использования вычислительных мощностей	Конкурирующие организации	Внешний	Н2
		Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Н1

Таблица 5

Номер УБИ	Наименование УБИ	Категория нарушителя и его возможности	Нарушенное свойство информации
УБИ.006	Угроза внедрения кода или данных	Внешний нарушитель с низким потенциалом	К, Ц, Д
УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации	Внешний нарушитель с низким потенциалом Внутренний нарушитель с низким потенциалом	К
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Внутренний нарушитель с низким потенциалом Внешний нарушитель со средним потенциалом	К, Ц, Д
УБИ.038	Угроза исчерпания вычислительных ресурсов хранилища больших данных	Внутренний нарушитель с низким потенциалом	Д
УБИ.060	Угроза неконтролируемого уничтожения информации хранилищем больших данных	Внутренний нарушитель с низким потенциалом	Ц, Д
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Внутренний нарушитель с низким потенциалом	К, Ц
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Внешний нарушитель с низким потенциалом Внутренний нарушитель с низким потенциалом	К
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Внешний нарушитель с низким потенциалом Внутренний нарушитель с низким потенциалом	Ц, Д
УБИ.088	Угроза несанкционированного копирования защищаемой информации	Внешний нарушитель с низким потенциалом Внутренний нарушитель с низким потенциалом	К, Ц



УБИ.091	Угроза несанкционированного удаления защищаемой информации	Внешний нарушитель с низким потенциалом Внутренний нарушитель с низким потенциалом	Д
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	Внешний нарушитель с низким потенциалом	К
УБИ.109	Угроза перебора всех настроек и параметров приложения	Внешний нарушитель со средним потенциалом Внутренний нарушитель со средним потенциалом	Ц, Д
УБИ.127	Угроза подмены действия пользователя путём обмана	Внешний нарушитель со средним потенциалом	К, Ц, Д
УБИ.139	Угроза преодоления физической защиты	Внешний нарушитель со средним потенциалом	К, Ц, Д
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	Внешний нарушитель с низким потенциалом Внутренний нарушитель с низким потенциалом	КБ Д
УБИ.157	Угроза физического вывода из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель с низким потенциалом	Ц, Д
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов	Внутренний нарушитель со средним потенциалом	К, Ц, Д
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Внутренний нарушитель с низким потенциалом	К, Ц, Д
УБИ.169	Угроза наличия механизмов разработчика	Внутренний нарушитель со средним потенциалом	К, Ц, Д
УБИ.175	Угроза «фишинга»	Внешний нарушитель с низким потенциалом	К
УБИ.179	Угроза несанкционированной модификации защищаемой информации	Внешний нарушитель с низким потенциалом Внутренний нарушитель с низким потенциалом	Ц

УБИ.180	Угроза отказа подсистемы обеспечения температурного режима	Внутренний нарушитель с низким потенциалом Внешний нарушитель со средним потенциалом	Д
УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Внешний нарушитель со средним потенциалом	К, Ц
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Внутренний нарушитель со средним потенциалом	К