ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ГЕОДЕЗИИ И КАРТОГРАФИИ

Отчет по заданию ФСТЭК

Вариант №13

Выполнил:
Студент 2021-ФГиИБ-ИБ-2б
Алексеев Дмитрий Игоревич
Иманаев Данила Иванович

Москва 2023

Роли пользователей в системе BitWarden:

1. **Пользователь:**

   Самый низкий уровень доступа. Подключение из внутренней сети к веб интерфейсу. Пользователи имеют доступ к своим паролям, но не к чужим.

2. **Администратор информационной системы (Админ ИС):**

   Ответственные за общее управление и настройку самой системы BitWarden.
   - Обновление BitWarden.
   - Управление пользователями и их ролями.
   - Мониторинг производительности и общего состояния системы.
   - Резервное копирование данных.

3. **Администратор информационной безопасности (Админ ИБ):**

   Занимается обеспечением безопасности системы и данных в BitWarden.
   - Настройка и мониторинг системы безопасности.
   - Реагирование на инциденты безопасности и расследование инцидентов.
   - Обеспечение соответствия системы нормативам и стандартам безопасности.
   - Управление аутентификацией и авторизацией.
   - Обеспечение безопасности передачи данных, включая протоколы шифрования.

Опросник НП: (Выполнил: Алексеев Дмитрий)

№	Наименование	Эксперт Алексеев Д.И.	Эксперт Иманаев Д.И.	Эксперт Богатова Е.Р.
У1	Угроза жизни или здоровью			Низкая
	Унижение достоинства личности	Высокая	Высокая	Средняя
	Нарушение свободы, личной неприкосновенности	Высокая	Высокая	Средняя
	Нарушение неприкосновенности частной жизни	Высокая	Высокая	Средняя
	Нарушение личной, семейной тайны, утрата чести и доброго имени	Высокая	Средняя	Средняя
	Нарушение тайны переписки, телефонных переговоров, иных сообщений	Высокая	Высокая	Средняя
	Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах	Высокая	Высокая	Средняя
	Финансовый, иной материальный ущерб физическому лицу	Средняя	Низкая	Средняя
	Нарушение конфиденциальности (утечка) персональных данных	Высокая	Высокая	Средняя
	«Травля» гражданина в сети «Интернет»	Низкая	-	Низкая
	Разглашение персональных данных граждан	Низкая	-	Низкая

У2	Нарушение законодательства Российской Федерации	Средняя	Низкая	Средняя
	Потеря (хищение) денежных средств	Низкая	Низкая	-
	Недополучение ожидаемой (прогнозируемой) прибыли			
	Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций	Средняя	-	Средняя
	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 управляемого объекта и/или процесса	Средняя	Высокая	Средняя
	Срыв запланированной сделки с партнером	Низкая	-	Низкая
	Необходимость дополнительных (незапланированных) затрат на восстановление деятельности	Средняя	Низкая	Средняя
	Потеря клиентов, поставщиков	Низкая	Низкая	Средняя
	Потеря конкурентного преимущества	-	Низкая	Средняя
	Невозможность заключения договоров, соглашений	-	Низкая	Средняя
	Нарушение деловой репутации. Снижение престижа	Средняя	Средняя	Средняя
	Дискредитация работников	Средняя	Средняя	Средняя
	Утрата доверия	Высокая	Высокая	Средняя
	Причинение имущественного ущерба	Низкая	Низкая	Средняя
	Неспособность выполнения договорных обязательств			
	Невозможность решения задач (реализации функций) или снижение	Средняя	Средняя	-

	эффективности решения задач (реализации функций)			
	Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций)	Высокая	Средняя	Средняя
	Принятие неправильных решений			
	Простой информационной системы или сети	Низкая	-	Средняя
	Публикация недостоверной информации на веб-ресурсах организации	Высокая	Высокая	Средняя
	Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением			
	Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени			
	Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)	Высокая	Высокая	Средняя

У3	Причинение ущерба жизни и здоровью людей.			
	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения			
	Прекращение или нарушение функционирования объектов транспортной инфраструктуры			
	Прекращение или нарушение функционирования государственного органа в частиневыполнения возложенной на него функции(полномочия)			
	Прекращение или нарушение функционирования сети связи			
	Отсутствие доступа к государственной услуге		Низкая	
	Нарушение условий международного договора Российской Федерации, срывпереговоров или подписания планируемого кзаключению международного договораРоссийской Федерации			
	Снижение уровня доходагосударственной корпорации, государственнойорганизации или организации с государственнымучастием			
	Возникновение ущерба бюджетам Российской Федерации.			
	Прекращение или нарушениепроведения клиентами операций по банковскимсчетам и (или) без открытия банковского			

	счетаили операций в системно значимой кредитнойорганизации, оператором услуг платежнойинфраструктуры системно и (или) социальнозначимых платежных систем, системно значимой инфраструктурной организацией финансового рынка			
	Вредные воздействия на окружающую среду	Низкая		
	Прекращение или нарушение функционирования пункта управления (ситуационногоцентра).			
	Снижение показателей государственного оборонного заказа.			
	Прекращение или нарушение функционирования информационной системы вобласти обеспечения обороны страны, безопасностигосударства и правопорядка			
	Нарушение законодательства Российской Федерации	Низкая	Низкая	Средняя
	Публикация недостоверной социально значимой информации на веб-ресурсах,которая может привести к социальной напряженности, паникесреди населения и др.			
	Нарушение штатного режимафункционирования автоматизированной системыуправления и управляемого объекта и/илипроцесса, если это ведет к выводу из строя технологических			

	объектов,их компонентов.			
	Нарушение выборного процесса			
	Отсутствие возможности оперативного оповещения населения о чрезвычайной ситуации			
	Организация пикетов, забастовок,митингов и других акций	Низкая	Средняя	-
	Массовые увольнения			
	Увеличение количества жалоб ворганы государственной власти или органыместного самоуправления			
	Появление негативных публикацийв общедоступных источниках	Средняя	Высокая	Средняя
	Создание предпосылок к внутриполитическому кризису			
	Доступ к персональным даннымсотрудников органов государственной власти,уполномоченных в области обеспечения обороны,безопасности и правопорядка, высшихдолжностных лиц государственных органов и другихлиц государственных органов.	Низкая		
	Доступ к системам и сетям с цельюнезаконного использования вычислительныхмощностей			
	Использование веб-ресурсовгосударственных органов для распространения иуправления вредоносным программным обеспечением			
	Утечка информации ограниченного доступа	Средняя	Высокая	Средняя
	Непредоставление государственных услуг			Средняя

Опросник НП с оценками экспертов: (Выполнил: Алексеев Дмитрий)

№	Наименование	Эксперт Алексеев Д.И.	Эксперт Иманаев Д.И.	Эксперт Богатова Е.Р.	Оценка
У1	Унижение достоинства личности	Высокая	Высокая	Средняя	7.6
	Нарушение свободы, личной неприкосновенности	Высокая	Высокая	Средняя	7.6
	Нарушение неприкосновенности частной жизни	Высокая	Высокая	Средняя	7.6
	Нарушение личной, семейнойтайны, утрата чести и доброго имени	Высокая	Средняя	Средняя	6.3
	Нарушение тайны переписки, телефонных переговоров, иных сообщений	Высокая	Высокая	Средняя	7.6
	Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах	Высокая	Высокая	Средняя	7.6
	Финансовый, иной материальныйущерб физическому лицу	Средняя	Низкая	Средняя	4
	Нарушение конфиденциальности (утечка) персональных данных	Высокая	Высокая	Средняя	7.6
	«Травля» гражданина в сети «Интернет»	Низкая	-	Низкая	1.3
	Разглашение персональных данных граждан	Низкая	-	Низкая	1.3

У2	Нарушение штатного режима функционирования автоматизированной системыуправления и управляемого объекта и/или процесса	Средняя	Высокая	Средняя	6.3
	Срыв запланированной сделки с партнером	Низкая	Низкая	-	1.3
	Необходимость дополнительных (незапланированных) затрат на восстановление деятельности	Средняя	Низкая	Средняя	4
	Потеря клиентов, поставщиков.	Низкая	Низкая	Средняя	3
	Потеря конкурентного преимущества	-	Низкая	Средняя	2.3
	Невозможность заключения договоров, соглашений	-	Низкая	Средняя	2.3
	Нарушение деловой репутации. Снижение престижа	Средняя	Средняя	Средняя	5
	Дискредитация работников	Средняя	Средняя	Средняя	5
	Утрата доверия	Высокая	Высокая	Средняя	7.6
	Причинение имущественного ущерба	Низкая	Низкая	Средняя	4
	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)	Средняя	Средняя	-	3.3
	Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций)	Высокая	Средняя	Средняя	6.3
	Простой информационной системы или сети	Низкая	-	Средняя	2.3
	Публикация	Высокая	Высокая	Средняя	7.6

	недостоверной информации на веб-ресурсах организации				
	Нарушение законодательства Российской Федерации	Средняя	Низкая	Средняя	4
	Потеря (хищение) денежных средств	Низкая	Низкая	-	1.3
	Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций	Средняя	-	Средняя	3.3
	Утечка конфиденциальной информации (коммерческой тайны, секретовпроизводства (ноу-хау) и др.)	Высокая	Высокая	Средняя	7.6

У3	Нарушение законодательства Российской Федерации	Низкая	Низкая	Средняя	3
	Появление негативных публикаций в общедоступных источниках	Средняя	Высокая	Средняя	6.3
	Утечка информации ограниченного доступа	Средняя	Высокая	Средняя	6.3
	Организация пикетов, забастовок,митингов и других акций	Низкая	Средняя	-	

Пример оценки целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации (для государственной информационной системы)

(Выполнил Иманаев Д.И)

	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**	
Специальные службы иностранных государств	-	-	-	-
Террористические, экстремистские группировки	-	-	+ (провокация общественности)	У3 (организация митингов, забастовок из-за публикаций недостоверной информации)

Продолжение таблицы 7.1

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**	
Преступные группы (криминальные структуры)	-	+ (Получение выгоды,шантаж)	+ (провокация общественности)	У2 (нарушение деловой репутации, публикация недостоверной информации на веб-ресурсах организации, причинение имущественного ущерба)

Отдельные физические лица (хакеры)	+ (желание самореализоваться)	+ (получение финансовой выгоды за счет кражи и коммерческой тайны)	-	У1 (Унижение достоинства личности, Нарушение тайны переписки, телефонных переговоров, иных сообщений) У2 (утечка коммерческой тайны; потеря клиентов, утрата доверия)
Конкурирующие организации	-	+ (Получение конкурентных преимуществ)	-	У2 Нарушение деловой репутации. Снижение престижа
Разработчики программных, программно-аппаратных средств	-	-	-	-
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	-	-	-	-
Поставщики вычислительных услуг, услуг связи	-	-	-	-

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.)	-	-	-	-
Авторизованные пользователи систем и сетей	+ (непреднамеренные, неосторожные или неквалифицированные действия)	-	-	У1 (Нарушение тайны переписки,телефонных переговоров, иных сообщений)
Системные администраторы и администраторы безопасности	+ (месть за ранее совершенные действия)	+ (любопытство или желание самореализации)	-	У1 (финансовый, иной материальный ущерб физическим лицам) У2 (Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций))

Бывшие (уволенные) работники (пользователи)	-	-	-	-

Определения актуальных нарушителей при реализации угроз безопасности информации и соответствующие им возможности
(Выполнил Иманаев Д.И.)

№ п/п	Виды риска (ущерба) и возможные негативные последствия*	Виды актуального нарушителя**	Категория нарушителя	Уровень возможностей нарушителя
1	У1: Унижение достоинства личности, Нарушение тайны переписки, телефонных переговоров, иных сообщений, финансовый, иной материальный ущерб физическим лицам	Отдельные физические лица (хакеры)	Внешний	Н2
		Авторизованные пользователи системи сетей	Внутренний	Н2
		Системные администраторы и администраторы безопасности	Внутренний	Н2
	У2: утечка коммерческой тайны; необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций), нарушение деловой репутации, публикация недостоверной информации на веб-ресурсах организации, причинение имущественного ущерба, потеря клиентов, утрата доверия, нарушение деловой репутации, снижение престижа	Преступные группы (криминальные структуры)	Внешний	Н3
		Отдельные физические лица (хакеры)	Внутренний	Н2
		Системные администраторы и администраторы безопасности	Внутренний	Н2
		Конкурирующие организации	Внешний	Н2
3	У3: организация митингов, забастовок из-за публикаций недостоверной информации	Террористические, экстремистские организации	Внешний	Н3

Перечень всех УБИ, которые потенциально могут существовать: (Выполнил: Алексеев Дмитрий)

Номер УБИ	Наименование УБИ	Категория нарушителя и его возможности	Какое свойство информации нарушает
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.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Внешний нарушитель с низким потенциалом Внутренний нарушитель с низким потенциалом	К, Ц, Д
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Внешний нарушитель с низким потенциалом Внутренний нарушитель с низким потенциалом	К, Д
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
УБИ.091	Угроза несанкционированного удаления защищаемой информации	Внешний нарушитель с низким потенциалом Внутренний нарушитель с низким потенциалом	Д
УБИ.133	Угроза получения сведений о владельце беспроводного устройства	Внешний нарушитель с низким потенциалом	К
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	Д
УБИ.152	Угроза удаления аутентификационной информации	Внешний нарушитель с низким потенциалом Внутренний нарушитель с	К, Ц, Д

		низким потенциалом	
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель с низким потенциалом	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.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Внешний нарушитель со средним потенциалом	К, Ц, Д
УБИ.197	Угроза хищения аутентификационной информации из временных файлов cookie	Внешний нарушитель со средним потенциалом	К
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Внешний нарушитель со средним потенциалом	Ц
УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Внешний нарушитель со средним потенциалом	К
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением	Внутренний нарушитель с низким потенциалом	К, Ц

	администрирования информационных систем		