Правительство Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

(НИУ ВШЭ)

ОТЧЕТ

ПО САМОСТОЯТЕЛЬНОЙ РАБОТЕ

по дисциплине «Основы кибербезопасности»

Студентка гр. БПИ245
Горбачева Маргарита
Валерьевна
«26» февраля 2026 г.

Руководитель
_____ Д.А. Белявский
«____»_____2026г.

Москва, 2026

Организация и выбранная Информационная Система (ИС)

1. Организация – АО "РТКОММ.РУ"

2. Выбранная информационная система - система контроля защищенности и соответствия стандартам информационной безопасности «MaxPatrol».

Программное обеспечение (ПО) для выбранной ИС:

1. СУБД Microsoft SQL Server 2008
2. Microsoft Exchange Server 2007
3. Cisco PIX (Private Internet Exchange)
4. JunOS
5. OpenSSH

Таблица с расчетом рисков

1. СУБД Microsoft SQL Server

Риск	Угроза, с помощью которой м.б. реализована уязвимость	Программное обеспечение (ПО)	Уязвимость(номер и описание)	Руязвимости	Ругрозы	D	R
Риск удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	Microsoft SQL Server 2008	BDU:2022-04046 Уязвимость реализации элемента управления «TabStrip» компонента MSCOMCTL.OCX пакета программ Microsoft Office, системы управления реляционными базами данных Microsoft SQL Server, программного средства для систем электронной коммерции Microsoft Commerce Server, среды разработки систем баз данных Microsoft Visual FoxPro связана с ошибками управления генерацией кода. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код с	=9,6/10= 96%	75%	2000000	1440000

			помощью специально созданного вредоносного файла или специально созданной вредоносной ссылки				
Риск подмены доверенного пользователя	УБИ.128: Угроза подмены доверенного пользователя	Microsoft SQL Server 2008	BDU:2024-00281 Уязвимость библиотек Microsoft.Data.Sqlclient (MDS) и System.Data.Sqlclient (SDS) программных платформ Microsoft .NET Framework и .NET связана с ошибками в настройках безопасности. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, обойти ограничения безопасности и реализовать атаку типа «человек посередине»	=7,1/10= 71%	100%	2000000	1420000
Риск повышения привилегий	УБИ.122 Угроза повышения привилегий	Microsoft SQL Server 2008	BDU:2025-14157 Уязвимость системы управления базами данных Microsoft SQL Server связана с непринятием мер по защите структуры запроса SQL. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить привилегии	= 9,0/10= 90%	50%	2000000,0	900 000
Риск подбора пароля BIOS	УБИ.123: Угроза подбора пароля BIOS	Microsoft SQL Server 2008	BDU:2024-10172 Уязвимость компонента Native Client системы управления базами данных Microsoft SQL Server связана с переполнением буфера в динамической памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код	=10/10= 100%	25%	2000000,0	500000

Риск приведения системы в состояние «отказ в обслуживании»	УБИ.140: Угроза приведения системы в состояние «отказ в обслуживании»	Microsoft SQL Server 2008	BDU:2023-07050 Уязвимость системы управления базами данных Microsoft SQL Server связано с недостаточной проверкой вводимых данных. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании	=5,5/10= 55%	0%	2000000,0	0

2. Microsoft Exchange Server 2007

Риск	Угроза, с помощью которой м.б. реализована уязвимость	Программное обеспечение (ПО)	Уязвимость(номер и описание)	Руязвимости	Ругрозы	D	R
Риск подмены доверенного пользователя	УБИ.128: Угроза подмены доверенного пользователя	Microsoft Exchange Server 2007	BDU:2025-10169 Уязвимость почтового сервера Microsoft Exchange Server связана с недостаточной проверкой входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, раскрыть защищаемую информацию	=7,5/10= 75%	100%	2000000	1500000
Риск передачи данных по скрытым каналам	УБИ.111 Угроза передачи данных по скрытым каналам	Microsoft Exchange Server 2007	BDU:2025-10166 Уязвимость почтового сервера Microsoft Exchange Server связана с недостаточной проверкой входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить несанкционированный доступ к защищаемой информации	=6,5/10= 65%	75%	2000000	1065975
Риск несанкционированной подмены	УБИ.4: Угроза несанкционированной подмены	Microsoft Exchange Server 2007	BDU:2025-10168 Уязвимость почтового сервера Microsoft Exchange Server связана с неправильной обработкой дополнительного специального элемента.	=5,3/10= 53%	50%	2000000	530000

			Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, проводить спуфинг-атаки				
Риск межсайтовой подделки запроса	УБИ.042: Угроза межсайтовой подделки запроса	Microsoft Exchange Server 2007	BDU:2021-05631 Уязвимость почтового сервера Microsoft Exchange Server связана с непринятием мер по защите структуры веб-страницы. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, осуществлять межсайтовые сценарные атаки с помощью специально созданной вредоносной ссылки	=4,3/10= 43%	25%	2000000	215000
Риск повышения привилегий	УБИ.122 Угроза повышения привилегий	Microsoft Exchange Server 2007	BDU:2025-09477 Уязвимость почтового сервера Microsoft Exchange Server связана с недостатками процедуры аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии	=7,1/10= 71%	0%	2000000	0

3. Cisco PIX (Private Internet Exchange)

Риск	Угроза, с помощью которой м.б. реализована уязвимость	Программное обеспечение (ПО)	Уязвимость(номер и описание)	Руязвимости	Ругрозы	D	R
Риск утечки информации	УБИ.1 Угроза утечки информации	Cisco PIX (Private Internet Exchange)	BDU:2015-00151 Уязвимость программного обеспечения Cisco IPS, позволяющая злоумышленнику получить доступ к конфиденциальной информации	=9,2/10= 92%	100%	2000000	1840000
Риск утечки	УБИ.193:		BDU:2015-00127	=8,3/10=	75%	2000000	1245000

информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Cisco PIX (Private Internet Exchange)	Уязвимость программного обеспечения Cisco IPS, позволяющая злоумышленнику перехватить сессию	83%			
Риск несанкционированного доступа	УБИ.2 Угроза несанкционированного доступа	Cisco PIX (Private Internet Exchange)	BDU:2015-00170 Уязвимость в Cisco PIX Firewall позволяет злоумышленнику, действующему по принципу "человек посередине", перехватить VPN-сессию пользователя.	=6,4/10=64%	50%	2000000	640000
Риск повышения привилегий	УБИ.122 Угроза повышения привилегий	Cisco PIX (Private Internet Exchange)	BDU:2015-00147 Уязвимость существует в функции загружаемых списков ACL RADIUS в Cisco PIX и концентраторах VPN 3000, при создании списка управления доступом (ACL) на сервере CS ACS (Cisco Secure Access Control Server), из-за генерирования произвольного внутреннего имени для списка ACL, которое также используется в качестве скрытого имени пользователя и пароля. Эксплуатация данной уязвимости позволяет злоумышленникам, действующим удаленно, повысить уровень своих привилегий, получив имя пользователя из незашифрованной части сессии RADIUS, а затем при помощи пароля получив доступ к другому устройству, использующему CS ACS.	=7,5/10=75%	25%	2000000	375000
Риск приведения системы в состояние	УБИ.140: Угроза приведения системы в	Cisco PIX (Private Internet Exchange)	BDU:2015-00185 Уязвимость в системах Cisco PIX (с открытым портом telnet или SSH)	=2,9/10=29%	0%	2000000	0

«отказ в обслуживании»	состояние «отказ в обслуживании»		позволяет злоумышленникам вызвать отказ в обслуживании, используя попытки подключения к службам, осуществляемые с очень большой частотой.				

4. JunOS

Риск	Угроза, с помощью которой м.б. реализована уязвимость	Программное обеспечение (ПО)	Уязвимость(номер и описание)	Руязвимости	Ругрозы	D	R
Риск утечки информации	УБИ.1 Угроза утечки информации	JunOS	BDU:2025-00307 Уязвимость интерфейса командной строки (CLI) операционных систем Juniper Networks Junos OS связана с недостаточной защитой служебных данных. Эксплуатация уязвимости может позволить нарушителю несанкционированный доступ к защищаемой информации	=8,8/10= 88%	100%	2000000	1760000
Риск повышения привилегий	УБИ.122 Угроза повышения привилегий	JunOS	BDU:2025-08765 Уязвимость интерфейса командной строки (CLI) операционных систем Juniper Networks Junos OS и Junos OS Evolved связана с непринятием мер по нейтрализации специальных элементов. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии	=6,7/10= 67%	50%	2000000	1005000
Риск подбора пароля BIOS	УБИ.123: Угроза подбора пароля BIOS	JunOS	BDU:2026-00672 Уязвимость демона jdhcpd операционных систем Juniper Networks Junos OS и Junos OS Evolved связана с недостатками	=5,5/10= 55%	75%	2000000	825000

			разграничения доступа. Эксплуатация уязвимости может позволить нарушителю получить полный контроль над системой				
Риск приведения системы в состояние «отказ в обслуживании»	УБИ.140: Угроза приведения системы в состояние «отказ в обслуживании»	JunOS	BDU:2025-08757 Уязвимость демона Routing Protocol Daemon (RPD) операционных систем Juniper Networks Junos OS и Junos OS Evolved связана с отсутствием освобождения памяти после эффективного срока службы. Эксплуатация уязвимости может позволить нарушителю оказать воздействие на доступность устройства	=4,6/10= 46%	25%	2000000	230000
Риск приведения системы в состояние «отказ в обслуживании»	УБИ.140: Угроза приведения системы в состояние «отказ в обслуживании»	JunOS	BDU:2026-01769 Уязвимость системного демона chassisd операционной системы Juniper Networks Junos маршрутизаторов серий MX, SRX и EX связана с разыменованием нулевого указателей. Эксплуатация уязвимости может позволить нарушителю вызвать отказ в обслуживании	=4,6/10= 46%	0%	2000000	0

5. OpenSSH

Риск	Угроза, с помощью которой м.б. реализована уязвимость	Программное обеспечение (ПО)	Уязвимость(номер и описание)	Руязвимости	Ругрозы	D	R
Риск утечки информации	УБИ.1 Угроза утечки информации	OpenSSH	BDU:2023-02094 Уязвимость агента идентификационных ключей ssh-agent средства криптографической защиты OpenSSH связана с использованием памяти после её освобождения. Эксплуатация	=10/10= 100%	100%	2000000	2000000

			уязвимости может позволить нарушителю, действующему удаленно, оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации				
Риск межсайтовой подделки запроса	УБИ.042: Угроза межсайтовой подделки запроса	OpenSSH	BDU:2025-01959 Уязвимость компонента VerifyHostKeyDNS средства криптографической защиты OpenSSH связана с недостатками обработки ошибок при проверке ключа хоста. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, провести атаку межсайтового скриптинга (XSS)	=7,1/10= 71%	75%	2000000	646065
Риск несанкционированной подмены	УБИ.4: Угроза несанкционированной подмены	OpenSSH	BDU:2025-10810 Уязвимость сервера средства криптографической защиты OpenSSH связана с недостатками процедуры аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить атаку MITM	=3,7/10= 37%	50%	2000000	370000
Риск удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	УБИ.195: Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	OpenSSH	BDU:2025-12884 Уязвимость компонента ssh средства криптографической защиты OpenSSH связана с некорректной обработкой специальных элементов. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код	=3,6/10= 36%	25%	2000000	180000
Риск несанкционированного	УБИ.2 Угроза несанкционированного	OpenSSH	BDU:2025-04768 Уязвимость службы sshd средства	=4,3/10= 43%	0%	2000000	0

доступа	доступа		криптографической защиты OpenSSH связана с несоответствием заявленной в документации функциональности директивы DisableForwarding. Эксплуатация уязвимости может позволить нарушителю оказать воздействие на целостность защищаемой информации				

Анализ рисков(выводы)

1. Что нужно сделать в организации, чтобы снизить значение рисков?

   а) Изучив множество уязвимостей и угроз, на сайте БДУ ФСТЭК несколько раз “бросалась в глаза” фраза, что решить/устранить проблему можно регулярным обновлением ПО, с чем я очень согласна.

   б) Также хорошим советом будет регулярное обучение персонала, чтобы снизить вероятность “попасть на крючок” к социальной инженерии.

   в) Обязательно стоит не забывать создавать сильные пароли, тк множество уязвимостей было связано именно со слабыми паролями.

   г) Очень важно в принципе заниматься технической стороной безопасности, то есть устанавливать firewall’ы, заниматься шифрованием трафика и тп.

   д) Конечно, нужно регулярно заниматься проверкой систем и сканированием потенциальных уязвимостей.

2. Какой уровень рисков для организации может быть приемлемым?

   Полагаю, что около 300.000 рублей, если изучать мою ИС, которая изначально была не ультра-дорогой. Для более дорогих и крупных ИС, считаю, цена может быть порядка до 500.000-1000.000 рублей.

3. Какие действия должны предпринять разработчики ИС, чтобы снизить риски?

а) Регулярное тестирование и обновление ИС;

б) Использование безопасных библиотек и компонентов(в моих примерах были случаи уязвимостей, связанных с использованием “не тех” библиотек).

в) Управление памятью;

г) И в целом, как описывала в пункте 1 – очень важно в принципе заниматься технической стороной безопасности, то есть устанавливать firewall’ы, заниматься шифрованием трафика и тп.

д) Мониторить инциденты.