**Годишен отчет за дейността на**

**Дирекция „Мрежова и информационна сигурност“ (ДМИС) за периода**

**01.01.2021 г. -31.12.2021 г.**

Дирекция „Мрежова и информационна сигурност“ е част от специализираната администрация в състава на Държавна агенция „Електронно управление" (ДАЕУ), подпомагаща председателя в изпълнението на държавната политика в областта на мрежовата и информационната сигурност.

Чл. 21. (1) Дирекция "Мрежова и информационна сигурност" (МИС) подпомага председателя на Агенцията, като изпълнява функциите на:

1. Национален компетентен орган за всички административни органи, както и за лицата и организациите по чл. 4, ал. 1, т. 3 и 4 от Закона за киберсигурност;

2. Национално единно звено за контакт по смисъла на чл. 17 от Закона за киберсигурност;

3. Национален екип за реагиране при инциденти с компютърната сигурност по смисъла на чл. 19 от Закона за киберсигурност;

4. Секторен екип за реагиране при инциденти с компютърната сигурност за административните органи по смисъла на чл. 18 от Закона за киберсигурност.

(2) Дирекция "Мрежова и информационна сигурност" осъществява и следните дейности:

1. разработва методика и правила за извършване на оценка за съответствие с мерките за мрежова и информационна сигурност, определени с наредбата по чл. 3, ал. 2 от Закона за киберсигурност;

2. координира, организира и провежда международни и национални учения и тренировки в областта на мрежовата и информационната сигурност;

3. участва в изготвянето на отчет за състоянието и на годишен план за развитието и обновяването на информационните ресурси в администрацията и информационните ресурси на Единната електронна съобщителна мрежа на държавната администрация, както и за нуждите на националната сигурност;

4. изпълнява дейности, свързани с функционирането на Националната координационно-организационна мрежа за киберсигурност и на Националния киберситуационен център;

5. участва в подготовката на проекти на стратегически документи и на нормативни актове в областта на мрежовата и информационната сигурност;

6. уведомява и осъществява взаимодействие със съответните компетентни органи при установени случаи на компютърни престъпления.

Дирекцията е подчинена на председателя на ДА „Електронно управление" и непосредствено се ръководи от директор.

До 30.09.2021г. Дирекцията е структурирана в 2 отдела:

* Отдел „ЕРИКС“;
* Отдел „Политики в МИС“;

От 01.10.2021г. в Дирекцията се закрива отдел ПМИС, като служителите преминават в отдел ЕРИКС и се създава нов отдел „Оперативно наблюдение киберсигурност“

От 03.11.2021 г Дирекцията вече е структурирана в три отдела:

* Отдел ЕРИКС
* Отдел „Оперативно наблюдение киберсигурност“
* Отдел “Анализ в киберсигутността“
1. **ОТДЕЛ Екип за Реагиране при Инциденти с компютърната сигурност ( ЕРИКС ) или Computer security incident response team (CSIRT)**

**Общи задължения на отдела (от правилника на ДАЕУ):**

1. **Направление ПМИС (Политики за Мрежова и Информационна Сигурност)**

Направлението осъществява следните функции в рамките на отдела

1. Подпомага Председателя на ДА ЕУ при провеждане на държавната политика по отношение на мрежовата и информационната сигурност в съответствие със Закона за киберсигурност, Наредба за минимални изисквания за мрежова и информационна сигурност и други подзаконови нормативни актове към тях при разрешаване на инциденти по отношение на мрежовата и информационната сигурност;
2. Осъществява координация при изпълнението на политиките за мрежова и информационна сигурност, свързани с функционирането на електронното управление;
3. Поддържа регистър на операторите на съществени услуги и на доставчиците на цифрови услуги;
4. Участва при удостоверяване съответствието на информационните системи на административните органи с изискванията за мрежова и информационна сигурност, включително извършва предварителни сканирания за уязвимости по чл. 24 от Наредбата за минималните изисквания за мрежова и информационна сигурност с цел установяване на съответствие с изискванията на глава втора от Наредбата за минималните изисквания за мрежова и информационна сигурност;
5. Изготвя годишен отчет за състоянието на мрежовата и информационна сигурност и го предоставя на съвета по киберсигурност;
6. По указание на директора на дирекция МИС изготвя проекти на регулярни отчети, доклади, планове и др. свързани с дейността на дирекция МИС, подготвя презентации и отговори на запитвания от средствата за масова информация в областта на МИС;
7. Осъществява дейности по планиране, подготовка, организиране и провеждане на обучения със звената или служителите по информационна сигурност в структурите на публичната администрация, и на национални и международни тренировки и учения в областта на киберсигурността/МИС;
8. Осъществява дейности свързани със сигнализиране и предупреждение при възникване на кризисни ситуации в МИС, предоставяне на информация за атаки, вируси и уязвимости, които вече са се проявили, като се описват начините за предотвратяване и предпазване.
9. Оказва методическа помощ на субектите по чл.4, ал.1, т.3 и т.4 от ЗКС, при изграждане, внедряване и поддържане в актуално състояние на системи за управление сигурността на информацията, съгласно изискванията на националните и международно признати стандарти и добри практики в тази област Участва в разработването на съвети и насоки по внедряване на най-добрите практики в областта на МИС при субектите по чл.4, ал.1, т.3 и т.4 от ЗКС.
10. Участва в разработването на проектни предложения и изпълнява дейности по тяхната реализация.
11. Подготвя предложение до Председателя на ДА ЕУ за методически указания по чл.12, т.3 от ЗКС;
12. Следи специализирани източници на информация свързана с новооткрити уязвимост, вируси, заплахи, атаки, експлойти и техники за прилагането им. След анализиране и адаптирането им към условията на Р България, публикува новини, съвети и предупреждения на Портала за МИС.
13. Проучва за добри практики в национален и международен план в областта на МИС и ги разпространява сред субектите по чл.4, ал.1, т.3 и т.4 от ЗКС;
14. Следи за и разпространява информация относно нови технологии в МИС,
15. Осъществява връзки и сътрудничество с европейски и други международни структури и организации в областта на мрежовата и информационната сигурност;
16. Участва в организирането и провеждането на обучения с отговорниците по информационна сигурност в структурите на публичната администрация съвместно с другите отдели в дирекцията;
17. Изпълнява функциите на Секретариат на Междуведомствената оперативна група към председателя на ДАЕУ за реакция при масирани кибератаки и широкомащабни инциденти;
18. Подготвя проекти на стратегически документи и нормативни актове в областта на МИС;
19. Координира действията си с други външни национални компетентни органи, споделяйки опита и знанията на експерти в областта на МИС от цял свят;
20. Изпълнява функциите на **Национален компетентен орган (НКО)** за всички административни органи, както и за органи, както и за лицата и организациите по чл.4, ал.1, т.3 и 4 от ЗКС, както и за операторите на съществени услуги (ОСУ) в сектор „Инфраструктури на финансовите пазари“, за което включва следните задачи/дейности**:**
* Координира и контролира изпълнението на задачите, свързани с мрежовата и информационната сигурност на административните органи, както и за лицата и организациите по чл.4. ал.1, т.3 и 4. От ЗКС;
* Изготвя/приема, насоки относно обстоятелствата, при които субектите по чл.4, ал.1 от ЗКС са длъжни да уведомяват за инциденти;
* Участва при оценяването дали административните органи, лицата и организациите по чл.4, ал.1, т.3 и т.4 от ЗКС, както и за ОСУ в сектор „Инфраструктури на финансовите пазари“ изпълняват задълженията си по глава втора от ЗКС, както и въздействието на това изпълнение върху мрежовата и информационната сигурност;
* Съвместно с Агенцията на Европейския съюз за киберсигурност (ENISA) изготвя препоръки и насоки по отношение на техническите области, които да се вземат предвид във връзка с използването на европейските или международните стандарти и спецификации от значение за мрежовата и информационната сигурност;
* Със съдействието на Агенцията на Европейския съюз за киберсигурност (ENISA) изготвя препоръки и насоки, свързани с използването на вече съществуващите стандарти, включително националните, с цел еднаквото прилагане на глава втора от ЗКС;
* Изисква при необходимост от административните органи, от лицата и организациите по чл.4, ал.1, т.3 и 4 от ЗКС и от ОСУ в сектор „Инфраструктури на финансовите пазари“:
	+ информация, необходима за оценка на мрежовата и информационната им сигурност, включително съществуващи политики за сигурност, резултати от одити на мрежовата и информационната сигурност, когато са извършени от друг квалифициран одитор, и доказателствата, на които те се основават;
	+ доказателства за ефективно изпълнение на препоръките от одити на мрежовата и информационната им сигурност;
* След оценяването на информацията или на доказателствата по чл.5 дава при необходимост задължителни указания за отстраняване на установените пропуски в изпълнението на изискванията, предвидени в глава втора от ЗКС.
* Оказва съдействие на Националното единно звено за контакт при изпълнение на функциите му по чл.17, ал.2, 3, 4 и 7 от ЗКС.
* Сътрудничи си с органите за защита на личните данни при работа по инцидентите, които водят до нарушение на сигурността на лични данни.

1. Изпълнява функциите на **Национално единно звено за контакт,** което включва следните задачи/дейности:
* Координира въпросите, свързани с мрежовата и информационната сигурност, и въпросите, свързани с трансграничното сътрудничество със съответните органи в други държави – членки на Европейския съюз.
* Предоставя на всеки две години на Европейската комисия информация относно последователността на подходите за определянето на операторите на съществени услуги, която включва:
	+ националните мерки, чрез които са определени операторите на съществени услуги;
	+ списък на съществените услуги;
	+ броя на операторите на съществени услуги, определени за всеки сектор в приложение № 1, и тяхното значение за този сектор;
	+ праговете, когато има такива, за определяне на минималното ниво на доставените услуги спрямо броя ползватели, разчитащи на тях;
	+ значението на конкретния оператор на съществени услуги за поддържане на достатъчно ниво на услугата предвид наличието и на други възможности за предоставяне на тази услуга.
* Уведомява Европейската комисия за:
	+ обхвата на задачите на екипите за реагиране при инциденти с компютърната сигурност по чл.18 и 19 от ЗКС, както и за съществените елементи от тяхната процедура за предприемане на действия при инциденти, след тяхното създаване или при изменение на статута или процедурите им;
	+ приетата Национална стратегия за мрежова и информационна сигурност в тримесечен срок от приемане й.
* При трансграничен инцидент уведомява националното единно звено за контакт на другата засегната държава – членка на Европейския съюз, когато е постъпило искане по чл.19, ал.2, т.9 от ЗКС от Националния екип за реагиране при инциденти с компютърната сигурност.
* Представя веднъж годишно обобщен доклад до Групата за сътрудничество относно получените уведомления по чл.21, ал.3, чл.22, ал.2, чл.23, ал.2 и чл.25, ал.3 от ЗКС, естеството на инцидентите и действията, предприети за разрешаването им.
* Изисква от националните компетентни органи информацията по ал.3 и ал.4, т.1 от ЗКС, а от Националния екип за реагиране при инциденти с компютърната сигурност – информацията по ал.7 от ЗКС при необходимост.
* В случай на необходимост осъществява сътрудничество със съответните правоприлагащи органи и с Комисията за защита на личните данни
1. Организира и участва в национални и международни конференции.

**През изминалата 2021г. в това направление бяха извършени следните дейности:**

* Беше актуализирана националната стратегия за киберсигурност „КИБЕРУСТОЙЧИВА БЪЛГАРИЯ 2023”, приета с Решение №301/02.04.2021 на Министерски съвет
* Към националната стратегия бе изготвена и проект на пътна карта, публикувана на сайта на ДАЕУ за предварително съгласуване с други заинтересувани органи на държавната администрация
* Активно участва в дискусиите по приемане на Директива МИС2
* Участва в работните групи по приемане на ЗИД на ЗДОИ и ЗЕУ
* Актуализиране състава на Междуведомствена оперативна група за реагиране при кибератаки и мащабни инциденти, създадена със заповед № ДАЕУ-4869/22.03.2021 г. и организиране и провеждане на 3 броя заседания и тренировки, във връзка с провеждането на парламентарни и президентски избори, за предоставяне на инструкции на членовете на групата при евентуални кибератаки
* Подготовка и подкрепа на заседанията на МВОГ съгласно Заповед №Р-118/27.07.2021 на Министър-председателя на Република България, изготвяне на анализ и насоки за изграждане на Интегрирана Национална Система за Киберсигурност на Република България
* Активно участва в работата по програмните документи на ПНИИДИТ
* Бяха организирани и проведени следните обучения:
* Два броя с отговорниците по МИС на тема приложение на Наредбата за минималните изисквания за мрежова и информационна сигурност
* Два броя с ГД КАНДЕ, което включваше напътствия при одит по НМИМИС, Процес по осъществяване на проверки съгласно чл.12, т.6 от ЗКС и разяснения по чл.24 и чл.25 от НМИМИС
* Поддържа в актуално състояние регистър на операторите на съществени услуги и на доставчиците на цифрови услуги
* По чл 36. Ал. 4 от НМИМИС, съгласно утвърдената годишна програма за 2021 са проверени следните администрации:
* Комисия за финансов надзор
* Държавна агенция държавен резерв и военновременни запаси
* Държавна комисия по стоковите борси и тържищата
* Община Първомай
* Български институт по метрология
* официалния сайт на ДАЕУ - е-gov.bg
* портала на ДАЕУ - EGOV.bg
* Обобщени и анализирани резултати от "Методика и правила за извършване на оценка за съответствието с мерките за МИС" - анкетите за 17 администрации:
* Държавна агенция "Архиви"
* Комисия за финансов надзор
* Общинска администрация Сливен
* Община Каварна
* Община Сандански
* Агенция за ядрено регулиране
* Държавна агенция "Държавен резерв и военновременни запаси"
* Община Първомай
* Държавна комисия по стоковите борси и тържищата
* Изпълнителна агенция по лекарствата
* Българска агенция по безопасност на храните
* Комисия за регулиране на съобщенията
* Община Димитровград
* Община Исперих
* Български институт по метрология
* Изпълнителна агенция по горите
* Областна администрация София
* В проверяваният период не е оказвано съдействие на Националното единно звено за контакт при изпълнение на функциите му по чл.17, ал.2, 3, 4 и 7 от ЗКС
* НКО е в близко сътрудничество с органите за защита на личните данни при работа по инцидентите, които водят до нарушение на сигурността на лични, каквито в проверявания период не са възникнали.
* Проверените технически спецификации са 80 броя, а проектните предложения – 62 броя
* Проверените проектни предложения във връзка с Актуализираната пътна карта за изпълнение на Актуализираната Стратегия за развитие на електронното управление за периода 2022-2025 г - над 60 броя
* Подготовка на проект на РМС за определяне Национален координационен център, според РЕГЛАМЕНТ (ЕС) 2021/887 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 20 май 2021 година за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове;
* Съгласуване на РМС №544 от 23 юли 2021 г. на основание член 58, параграфи 1 и 2 от Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019, за определяне на председателя на ДАЕУ за Национален орган за сертифициране на киберсигурността на информационните и комуникационните технологии.
1. **Направление НЕРИКС „CSIRT”(Computer Security Incident Response Team)**

Направлението осъществява следните функции в рамките на отдела:

1. Осъществява функциите на „гореща линия“ по съществуващите комуникационни канали, със субектите по чл.4, ал.1, т.3 и т.4 от ЗКС, с мрежата на европейските CSIRTs други национални и международни центрове и организации в при реакция на инцидента в областта на МИС.
2. Координира и участва в изграждането, експлоатирането, поддържането и развитието на:
	* Национална мрежа на екипите за реагиране при инциденти с компютърната сигурност;
	* НКОМКС;
	* НКСЦ;
	* Зала за национални и международни киберучения;
	* Лаборатория за зловреден код и лаборатория за анализи на артефакти от инциденти;
	* Център за наблюдения и за реакция при инциденти с компютърната сигурност;
	* Система за мониторинг и съхранение на документи свързани с МИС.
3. Осъществява дейности свързани с управление на инциденти в МИС, които се изразяват в следното;
	* Изучава наличната информация, помощните доказателства и артефакти, свързани с инцидента или събитието;
	* Идентифицира обхвата на инцидента, степента на вреда, причинена от него, както и характера на инцидента и наличните стратегии за реакция или за заобикаляне или предотвратяване;
	* Събиране, запазване, документиране и анализ на доказателства от атакувана компютърна система за определяне на промените в системата и за подпомагане на възстановяването на събития, водещи до пробива;
	* Проследяване на произхода на нарушителя или идентифицирането на системите, до които има достъп. Тази дейност включва проследяване на начина, по който нарушителя е влязъл в засегната система и свързаните мрежа, кои системи са били използвани за получаване на достъп, къде е възникнала атаката, и кои други системи и мрежи са били използвани като част от атаката. Включва и опит за идентифициране на нарушителя анализиране на инциденти и събития.
	* Предприемане на действия за разрешаване на възникналите инциденти, за предпазване на системи и мрежи, засегнати или заплашени от нежелани атаки; при необходимост асистиране за възстановяване на системите;
	* Предлагане на решения и стратегии за намаляване на рисковете, в резултат на вече случили се подобни събития;
	* Предоставяне на информация за актуализация и обновяване на системите; разработване на други отговори или алтернативни стратегии за разрешаване на възникнали проблеми;
	* Асистиране при разрешаването на инциденти от страна на други европейски и световни CERTs организации.
4. При необходимост оказва помощ при справяне с инциденти като осигурява съдействие в помощ на ползвателите на услугите при възстановяване на системи в следствие на възникване на инциденти.
5. Осъществява дейности свързани с управление на уязвимости. Определя подходящи действия за смекчаване или поправяне на уязвимостите при тяхното откриване.
6. Осъществява дейности свързани с управление на артефакти. Определя правилните действия за откриване и премахване на артефакти от информационните системи, както и проактивните действия, които трябва да се предприемат за предпазване от инсталация на артефакти върху тези системи. Събира информация за копия на артефакти, използвани при дадена атака, както и разузнавателни действия свързани с откриване на методите за причиняване на нежелателни влияния върху системите. Извършва технически преглед и анализ на всеки артефакт, открит на дадена система.
7. Изготвя ежедневно Справки за дейностите на ЕРИКС.
8. Поддържат необходими за дейността си бази данни и статистически данни.
9. Уведомява и осъществява взаимодействие при необходимост с ГД БОП при установени случаи на компютърни престъпления и с ДАНС в случай на инциденти с мрежовата и информационна сигурност на стратегически обекти и дейности със значение за националната сигурност.
10. Поддържа и обновява списък с контактна информация за секторните ЕРИКС и отговорниците по МИС на административните органи и субектите по чл. 4, ал. 1, т. 3 и т. 4 от ЗКС.
11. Подпомага публични организации и институции да развиват своите умения в разрешаването на инциденти в МИС (дават насоки и предоставят информация за планиране и изграждане на звена за сигурност, създават взаимовръзки и стимулират дискутирането на проблеми помежду им), както и да повишават своята осведоменост по въпросите на МИС.
12. Осъществява контакти с мрежата на европейските CSIRTs, с други международните структури, с които взаимодейства CSIRT България. Осигурява непрекъснатата свързаност на CSIRT България с Екипа на НАТО за реакция при компютърни инциденти (NCIRC), в съответствие с MoU между България и НАТО.
13. Осъществява комуникации и връзки със служителите или звената по мрежова и информационна сигурност на административните органи и субектите по чл. 4, ал.1, т. 3 и т. 4 от ЗКС.
14. Осъществява дейности по отношение инфраструктура на дирекция МИС, в рамките на правомощията на дирекцията.
15. Изпълнява функцията на **Национален Екип за Реагиране при инциденти в компютърната сигурност (нЕРИКС; nCSIRT),** което включва следните задачи/дейности:
	* Действа като звено за контакт по въпроси, свързани с мрежовата и информационната сигурност на национално ниво и по оперативни въпроси на международно ниво;
	* Подпомага дейностите по създаването на секторните екипи за реагиране при инциденти с компютърната сигурност;
	* Участва в изграждането и дейностите на Националната мрежа на екипите за реагиране при инциденти с компютърната сигурност;
	* Обобщава и анализира предоставената информация от секторните екипи за реагиране при инциденти с компютърната сигурност и изготвя доклади в случай на необходимост;
	* Предоставя съвети и препоръки на органите на държавна власт, органите на местното самоуправление и юридическите лица, създадени със специален закон, по важни въпроси, свързани с мрежовата и информационната сигурност;
	* Оказва експертна подкрепа на административните органи и при изграждане, внедряване и поддържане в актуално състояние на системи за управление на информационната сигурност съгласно националните и международните стандарти в тази област;
	* Участва в разработването и тестването на национални и по линия на Европейския съюз и НАТО стандартни оперативни процедури;
	* При възникване на инциденти в мрежовата и информационната сигурност дава препоръчителни указания на административни органи, на националната компетентни органи и на секторните екипи за реагиране при инциденти с компютърната сигурност;
	* Информира незабавно Националното единно звено за контакт за уведомленията за трансгранични инциденти със значително увреждащо въздействие и за трансгранични инциденти със съществено въздействие, подадени съгласно този екип, и в случай на необходимост иска съдействие от Националното единно звено за контакт за тяхното разрешаване;
	* Поддържа база данни с обобщена статистическа информация за регистрираните инциденти в МИС получаване от секторните ЕРИКС на всеки три месеца/ с тримесечните им отчети;
	* Сътрудничи си с предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги за отстраняване на установени от него киберинциденти в техните мрежи и/или услуги.

16, Изпълнява функциите на **Секторен Екип за Реагиране при инциденти в компютърната сигурност за административните органи и субектите по чл.4, ал.1, т.3 и т.4 от ЗКС,** което включва следните задачи/дейности:

* + Екипът се създава в съответствие с методическите указания на Агенция на Европейския съюз за киберсигурност (ENISA).
	+ Осъществява дейността си в съответствие с процедури, утвърдени от председателя на ДАЕУ.
	+ Изпълнява реактивни, проактивни дейности и дейности по управление на качеството на сигурността в съответствие с регламентиращите и препоръчителните документи на Европейския съюз, с указанията на Агенцията на Европейския съюз за киберсигурност (ENISA) и с българското законодателство.
	+ Наблюдава инциденти в МИС на национално равнище.
	+ Подава ранни предупреждения, сигнали за тревога, съобщения и разпространява информация за инциденти и рискове сред съответните субекти.
	+ При поискване оказва методологическа помощ при разрешаване на инциденти.
	+ Осигурява динамичен анализ на рисковете и инцидентите и изготвя информация за текущата ситуация.
	+ Осъществява сътрудничество с частния сектор и с академичните среди.
	+ Разработва и споделя със секторните ЕРИКС:

(а) процедури за предприемане на действия при инциденти и рискове;

(б) схеми за класификация на инциденти, рискове и информация.

* + Информира незабавно НЕЗК за трансгранични инциденти, подадени съгласно ЗКС.
	+ На всеки три месеца изготвя обобщена статистическа информация относно регистрираните инциденти в мрежовата и информационната сигурност, засягащи административните органи и субектите о чл.4, ал.1, т.3 и т.4 от ЗКС.

**През изминалата 2021г. в това направление бяха извършени следните дейности:**

Във връзка с осъществяване на проактивни и реактивни дейности по управление на инциденти, уязвимости и артефакти в областта на мрежовата и информационна сигурност, по отношение на управлението на инциденти в МИС (Мрежова и информационна сигурност), бе организирано постоянно наблюдение и реакции при инциденти, като за периода са регистрирани и разрешени 2099 инцидента.

Таблицата показва сравнителен анализ на получените сигнали, засегнати IP адреси, изпратените писма и регистрираните инциденти за последните три години.

|  |  |  |  |
| --- | --- | --- | --- |
|  | 2021 | 2020 | 2019 |
| Получени сигнали | 4759 | 3451 | 3311 |
| Засегнати IP адреси | 276970 | 392283 | 2288293 |
| Изпратени мейли | 18103 | 18617 | 21883 |
| Регистрирани на сайта | 2099 | 2087 | 1919 |





* Предупреждения за актуализация на уязвими продукти редовно се публикуват на портала на CERT България, като за отчетния период са публикувани **205 бр. предупреждения, 5 бр. съвети и 39 бр. новини**.
* Изготвят се ежедневни справки за дейностите на CERT България, съдържащи вида и броя сигнали за нарушения в и от Българското Интернет пространство, които се предоставят при поискване и до други заинтересовани. Изготвят се ежемесечни информационни бюлетини за възможни заплахи, възникващи инциденти и добри практики в информационната сигурност, които се изпращат всеки месец до всички служители по мрежова и информационна сигурност, до конституентите на CERT България, както и заинтересовани организации.
* Изготвени и изпратени са подробни анализи за Pegasus Trojan и Ransomware.
* Сканиране за уязвимости на уебсайтовете на общините, което включва:
	+ Инсталиране на Web Security Map (софтуера на Internet Cleanup Foundation)
	+ Актуализиране на списъка с уебсайтовете на общините и проверка наличността на всички сайтове
	+ Въвеждане на уебсайтовете на всички общини в софтуера, конфигуриране за тип сканиране
	+ Задаване на периода на сканиране.
	+ Генериране, запазване и изпращане на докладите от резултатите от сканирането за всяка община.
* За безпроблемното протичане на изборите за 44, 45 и 46 Народно събрание, и избори за президент и вицепрезидент на Република България, които се проведат на 14.11.2021г., както и евентуален балотаж на 21.11.2021г, се организираха следните мероприятия и дейности:
* Изготвени и изпратени указания за повишаване на МИС;
* Организирано дежурство по време на изборите
* Тренировка по оповестяване и свикване на МВОГ
* Участва активно в:
* изготвяне на Методика за удостоверяване на съответствието на доставения тип техническо устройство за машинно гласуване с изискванията по чл.213, ал. 3 от Изборния кодекс и изискванията на Техническата спецификация по обществена поръчка № 04312-2020-0001
* изготвяне на Приложение 4 – Проверка на сигурността на ТУМГ
* Удостоверяване на ТУМГ
* Участва в национални и международни учения:
* Проверка на SOPex на CSIRT Network
* Lock Shield на НАТО
* Cyber Coalition на НАТО
* Няколкократни учения на мрежата CyCLONE

- Организира и участва в мероприятията посветени на Месеца на киберсиигурността

- Участва в изготвянето на „Оценка на заплахите от организирана престъпност в България“, към Центъра за изследване на демокрацията.

- Изготви и изпрати специални Указания за повишаване нивото на МИС при работа отдалечено с създалата се епидемиологична обстановка

- Изготви и изпрати указания и препоръки във връзка с пробив в сигурността на пощенските сървъри на Microsoft: Exchange Server 2013, Exchange Server 2016 и Exchange Server 2019

- Изготви и изпрати указания във връзка с уязвимостта Log4j

- Участва в заседанията на CSIRT Network, където е пълноправен член

- Ежедневно следи информацията свързана киберобстановката

1. **Отдел Оперативно наблюдение Киберсигурност – Security Operations Center ( SOC )**
2. Подпомага Председателя на ДА ЕУ при наблюдението и анализа на националното киберпространство;
3. По указание на директора на дирекция МИС изготвя проекти на регулярни отчети, доклади, планове и др. свързани с дейността на дирекция МИС, подготвя презентации и отговори на запитвания от средствата за масова информация в областта на МИС;
4. Събира, консолидира, обработва и анализира оперативна информация от информационни системи, мрежови потоци, журнални записи, сървъри-примамки и други средства за наблюдение на активностите и действията на потребители в киберпространството във връзка с подпомагане на функциите на Дирекция Мрежова и Информационна сигурност;
5. Изготвя и разпространява информация, включително и в машинно четим вид до заинтересуваните организации с цел превантивна защита от киберинциденти;
6. При идентифициране на киберинцидент незабавно уведомява отдел ЕРИКС и организациите, засегнати от киберинцидента. Уведомява и осъществява взаимодействие и със следните организации при необходимост:
	* с ГД БОП при установени случаи на компютърни престъпления;
	* с ДАНС в случай на инциденти с мрежовата и информационна сигурност на стратегически обекти и дейности със значение за националната сигурност;
	* С органите по защита на личните данни при инциденти, заплашващи сигурността на лични данни;
7. Осъществява дейности свързани със сигнализиране и предупреждение при възникване на оперативни кризисни ситуации в МИС, предоставяне на информация за атаки, вируси и уязвимости, които вече са се проявили, като се описват начините за предотвратяване и предпазване;
8. Участва в изграждането, подбора и оперирането и поддържането на технологичните инструменти, средства и платформи, необходими за осъществяването на дейността по оперативно наблюдение на събитията свързани с мрежова и информационна сигурност;
9. Участва в разработването на проектни предложения и изпълнява дейности по тяхната реализация.
10. Организира и участва в национални и международни конференции.
11. Осъществява дейности по планиране, подготовка, организиране и провеждане на обучения със звената или служителите по информационна сигурност в структурите на публичната администрация, и на национални и международни тренировки и учения в областта на киберсигурността/МИС;
12. Поддържа необходими за дейността си бази данни и статистически данни.

**През изминалата 2021г. в това направление бяха извършени следните дейности:**

1. Изграждане на софтуерна система, която обединява данните от разположените в мрежата на държавната администрация honeypots, както и развитие на спомената мрежа чрез добавяне на нови възли
2. Активно участие в работните групи то удостоверяване на ТУМГ
3. **Отдел Анализи в киберсигурността**
4. Подпомага Председателя на ДА ЕУ при анализа на информационни платформи, инструменти и системи, както и за спазването на нормативните изисквания при тяхната разработка;
5. По указание на директора на дирекция МИС изготвя проекти на регулярни отчети, доклади, планове и др., подготвя презентации и отговори на запитвания в областта на МИС;
6. Изгражда и поддържа ISAC ( Information Sharing and Analytics Center ) съгласно практиките на ENISA, който да предоставя централен ресурс за събиране на информация за киберзаплахи, както и позволяват двустранно споделяне на информация между частния и публичния сектор относно първопричини, инциденти и заплахи, както и споделяне на опит, знания и анализи;
7. Анализира, проверява, изпробва изходният код на информационни платформи, системи и инструменти във връзка с наличието на уязвимости, слабости и спазване на нормативни изисквания
8. Подпомагат проверките на съответствието на информационни системи спрямо изискванията на чл 58а от Закон за Електронното управление във всички фази на разработката на системите – проект, разработка, тестване, въвеждане в експлоатация и поддръжка
9. Разработват методически указания и подпомагат органите на държавната администрация за:
	* Изисквания за сигурни и устойчиви информационни системи
	* разработването на информационни системи, включително въвеждане на принципи за информационна сигурност на ниво дизайн и проект;
	* поддръжката и оперирането на информационни системи;
	* тестването на информационни системи и техни модули и компоненти по отношение на функционалност, устойчивост, производителност и уязвимости;
	* управлението на компонентите и библиотеките на информационните системи, които са създадени от трети страни;
10. Участва в изграждането, подбора и оперирането и поддържането на технологичните инструменти, средства и платформи, необходими за осъществяването на дейността по оперативно наблюдение на събитията свързани с мрежова и информационна сигурност;
11. Участва в разработването на проектни предложения и изпълнява дейности по тяхната реализация.
12. Организира и участва в национални и международни конференции.
13. Осъществява дейности по планиране, подготовка, организиране и провеждане на обучения със звената или служителите по информационна сигурност в структурите на публичната администрация, и на национални и международни тренировки и учения в областта на киберсигурността/МИС;
14. Поддържа необходими за дейността си бази данни и статистически данни.

**През изминалата 2021г. в това направление бяха извършени следните дейности:**

1. Анализ на предоставена от частна фирма методика и подход за оценка на рисковете по отношение на съответствие с НМИМИС и ЗКС
2. **Други дейности**

През отчетния период дирекцията продължава работата по проектите:

**Фонд „Вътрешна сигурност“:**

* [„Изграждане на елементи от национална система за киберсигурнoст“](https://e-gov.bg/wps/portal/agency/all-projects/projects-DAEU/%21ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8ziPQItHA39LYy8DVxNzAwCzcwcHU2dHY1Mg4z0w9EUuBhYGDh6-PiFWlq4GRo4m-hHEaPfAAdwNCBOPx4FUfiND9ePQrXC3S_IxSDQMcDXO8AjzNzMxAhdARYvErKkIDc0NMIg0xMABUAArQ%21%21/?1dmy&urile=wcm%3apath%3a%2Fdaeu%2Fsite%2Fall-projects%2Fprojects-DAEU%2Fprojects-mis%2FProject-cybersecurity)
* „Изграждане на Център за мониторинг и реакция на киберинциденти в стратегически обекти“

**Програма „Механизъм за свързване на Европа“:**

* [„Изграждане на капацитет и подобряване на услугите, предоставяни от CERT България “ /Capacity Building and Services Enhancement of CERT Bulgaria (CBSEC-BG)](https://e-gov.bg/wps/portal/agency/all-projects/projects-DAEU/%21ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8ziPQItHA39LYy8DVxNzAwCzcwcHU2dHY1Mg4z0w9EUuBhYGDh6-PiFWlq4GRo4m-hHEaPfAAdwNCBOPx4FUfiND9ePQrXC3S_IxSDQMcDXO8AjzNzMxAhdARYvErKkIDc0NMIg0xMABUAArQ%21%21/?1dmy&urile=wcm%3apath%3a%2Fdaeu%2Fsite%2Fall-projects%2Fprojects-DAEU%2Fprojects-mis-eu%2FCEF)

**Програма Хоризонт 2020:**

* [„FORESIGHT - Усъвършенствана симулационна платформа за киберсигурност за обучение в авиационната, морската и Powergrid средата](https://e-gov.bg/wps/portal/agency/all-projects/projects-DAEU/%21ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8ziPQItHA39LYy8DVxNzAwCzcwcHU2dHY1Mg4z0w9EUuBhYGDh6-PiFWlq4GRo4m-hHEaPfAAdwNCBOPx4FUfiND9ePQrXC3S_IxSDQMcDXO8AjzNzMxAhdARYvErKkIDc0NMIg0xMABUAArQ%21%21/?1dmy&urile=wcm%3apath%3a%2Fdaeu%2Fsite%2Fall-projects%2Fprojects-DAEU%2Fprograma-horizont%2FFORESIGHT)“. Техническият и финансов отчет за изпълнение на проекта за първите 18 месеца е приет от ЕК.
1. **Участие в работни групи за разработка и изменение на нормативни документи и комисии по обществени поръчки:**
* Участие в Работна група 17;
* Участие в работна група по подготовка на ЗИД на Закон за електронно управление.
* Работна група за изготвяне на проект на нова НОИИСРЕАУ и приложенията към нея. Наредбата и приложенията са изпратени към Междуведомствената група за съгласуване.;
* Участие в заседанията на Хоризонталната група по въпросите за киберсигурността на ЕК
* Участие в Групата за сътрудничество на ЕС
* Участие в CSIRT NETWORK

**С уважение,**

**Петър Кирков**

*Директор на дирекция ,,Мрежова и информационна сигурност”*